Axproo

Axproo Cyber Cloud
Version 9.0

GUIDE DU PARTENAIRE

Révision : 05/06/2020

Table des matières

1 À propos de ce document

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

Ce document décrit comment configurer et gérer les services disponibles dans Axproo Cyber Cloud.

2 À propos de Axproo Cyber Cloud

Axproo Cyber Cloud 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

2.1 Gestion des éléments et des quotas

Cette section décrit les éléments suivants :

- Quels sont les services, offres et éléments ?
- Comment les éléments sont-ils activés ou désactivés ?
- 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 ?

2.1.1 Services, offres et éléments

Services

Les services suivants sont disponibles dans Cyber Cloud de Axproo :

- **Cyber Protection**
- **File Sync & Share**
- **SPLA Cyber Infrastructure**

- **Notary**
- **Envoi de données physiques**

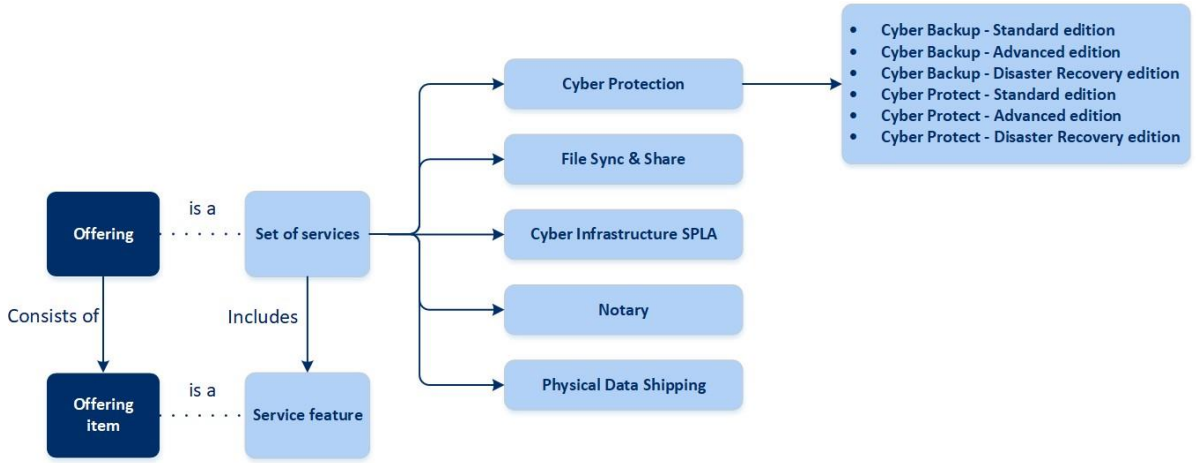
Vous pouvez définir les services qui seront disponibles pour vos partenaires et clients en les activant ou en les désactivant.

Offres et éléments

Cyber Cloud Axproo vous permet de personnaliser l'offre (l'ensemble des services et caractéristiques des services, appelés **Éléments**) que vous délivrez à vos clients et partenaires.

L'**offre** définit les services et fonctionnalités qui seront disponibles aux partenaires, aux clients et à leurs utilisateurs finaux dans le portail de gestion et les consoles de service. Toutes les fonctionnalités exclues de l'offre leur seront cachées.

Pour affiner davantage leurs offres, vous pouvez définir des quotas pour les éléments spécifiques.



Éditions du service Cyber Protection

Le service Cyber Protection possède six éditions qui déterminent les fonctionnalités proposées aux clients.

Édition	Description
Cyber Backup - Standard	Fonctionnalités : ▪ Fonctionnalité de sauvegarde et de restauration adaptée aux besoins des environnements de petite taille ▪ Fonctionnalités d'évaluation des vulnérabilités, d'installation à distance de base, et de protection basique contre le ransomware et le cryptominage ▪ Fonctionnalité d'installation à distance de base
Cyber Backup - Advanced	Fonctionnalités : ▪ Fonctionnalité de sauvegarde et de restauration dédiée à la protection des charges de travail avancées telles que les clusters Microsoft Exchange et Microsoft SQL conçus pour des environnements de grande taille ▪ Gestion de groupe et de plan ▪ Fonctionnalités d'évaluation des vulnérabilités, d'installation à distance, et de protection basique contre le ransomware et le cryptominage ▪ Fonctionnalité d'installation à distance avancée

Cyber Backup - Disaster Recovery	Fonctionnalités : ▪ Fonctionnalité de sauvegarde et de restauration dédiée à la protection des charges de travail avancées telles que les clusters Microsoft Exchange et Microsoft SQL conçus pour des environnements de grande taille ▪ Gestion de groupe et de plan ▪ Fonctionnalités d'évaluation des vulnérabilités, d'installation à distance de base, et de protection basique contre le ransomware et le cryptominage ▪ Fonctionnalité d'installation à distance avancée ▪ La fonctionnalité de reprise d'activité après sinistre est conçue pour les entreprises ayant des exigences élevées en matière d'objectif de temps de restauration
Cyber Protect – Standard	Fonctionnalités : ▪ Fonctionnalité de sauvegarde et de restauration adaptée aux besoins des environnements de petite taille ▪ Fonctionnalité d'installation à distance de base ▪ Fonctionnalités d'évaluation des vulnérabilités et de gestion des correctifs ▪ Fonctionnalité avancée de protection anti-malware et de protection Web ▪ Fonctionnalité de bureau à distance ▪ Fonctionnalité de contrôles de sécurité comme la gestion de Windows Defender ▪ Alertes basées sur les données du centre opérationnel de cyberprotection ▪ Fonctionnalité de découverte des données
Cyber Protect – Avancé	Fonctionnalités : ▪ Fonctionnalité de sauvegarde et de restauration dédiée à la protection des charges de travail avancées telles que les clusters Microsoft Exchange et Microsoft SQL conçus pour des environnements de grande taille ▪ Gestion de groupe et de plan ▪ Fonctionnalité d'installation à distance avancée ▪ Fonctionnalités d'évaluation des vulnérabilités et de gestion des correctifs ▪ Fonctionnalité avancée de protection anti-malware et de protection Web ▪ Fonctionnalité de bureau à distance ▪ Fonctionnalité de contrôles de sécurité comme la gestion de Windows Defender ▪ Alertes basées sur les données du centre opérationnel de cyberprotection ▪ Fonctionnalité de découverte des données

Cyber Protect – Plan de reprise d'activité après sinistre	Fonctionnalités : ▪ Fonctionnalité de sauvegarde et de restauration dédiée à la protection des charges de travail avancées telles que les clusters Microsoft Exchange et Microsoft SQL conçus pour des environnements de grande taille ▪ Gestion de groupe et de plan ▪ Fonctionnalité d'installation à distance avancée ▪ Fonctionnalités d'évaluation des vulnérabilités et de gestion des correctifs ▪ Fonctionnalité avancée de protection anti-malware et de protection Web ▪ Fonctionnalité de bureau à distance ▪ Fonctionnalité de contrôles de sécurité comme la gestion de Windows Defender ▪ Alertes basées sur les données du centre opérationnel de cyberprotection ▪ Fonctionnalité de découverte des données ▪ La fonctionnalité de reprise d'activité après sinistre est conçue pour les entreprises ayant des exigences élevées en matière d'objectif de temps de restauration

L'édition vous permet de différencier les offres de protection des données pour vos partenaires et clients, et de proposer les fonctionnalités de protection des données qui répondent à leurs besoins et à leur budget.

Vous pouvez décider des éditions qui seront disponibles pour votre partenaire en les désactivant lors de la création du partenaire. Chaque édition peut être ajustée en configurant les éléments.

Vous pouvez attribuer une édition par client. Par la suite, vous pouvez faire passer les clients d'une édition à une autre, à la demande.

2.1.2 Gestion des éditions du service Cyber Protection pour les partenaires

Désactivation des éditions pour vos locataires partenaires

Pour désactiver l'édition d'un locataire partenaire, accédez à **Clients** > **<particular_partner>** > onglet **Configurer** et désélectionnez l'édition. Saisissez votre identifiant pour confirmer la désactivation de l'édition.

Désactivation de l'édition Cyber Backup - Disaster Recovery

Les modifications suivantes auront une incidence sur le locataire sélectionné et ses locataires enfants qui disposaient de l'édition Cyber Backup - Disaster Recovery :

- L'édition Cyber Backup - Disaster Recovery deviendra indisponible.
- Tous les plans de protection seront révoqués, tous les appareils seront désinscrits et leurs sauvegardes seront supprimées.
- La fonctionnalité de reprise d'activité après sinistre va devenir indisponible : tous les serveurs de restauration, serveurs primaires et configurations de réseau pour reprise d'activité après sinistre ne seront plus disponibles ; les appliances VPN seront désinscrites ; les adresses IP publiques seront révoquées des serveurs dans le Cloud et les serveurs ne seront pas accessibles à partir d'Internet.

Désactivation de l'édition Cyber Backup - Advanced/Standard

Les modifications suivantes auront une incidence sur le locataire sélectionné et ses locataires enfants qui disposaient de l'édition Cyber Backup - Advanced/Standard :

- L'édition Cyber Backup -Advanced/Standard deviendra indisponible.
- Tous les plans de protection seront révoqués, tous les appareils seront désinscrits et leurs sauvegardes seront supprimées.

Désactivation de l'édition Cyber Protect - Disaster Recovery

Les modifications suivantes auront une incidence sur le locataire sélectionné et ses locataires enfants qui disposaient de l'édition Cyber Protect - Disaster Recovery :

- L'édition Cyber Protect - Disaster Recovery deviendra indisponible.
- Tous les plans de protection seront révoqués, tous les appareils seront désinscrits et leurs sauvegardes seront supprimées.
- Toutes les fonctionnalités de Cyber Protect seront désactivées.
- La fonctionnalité de reprise d'activité après sinistre va devenir indisponible : tous les serveurs de restauration, serveurs primaires et configurations de réseau pour reprise d'activité après sinistre ne seront plus disponibles ; les appliances VPN seront désinscrites ; les adresses IP publiques seront révoquées des serveurs dans le Cloud et les serveurs ne seront pas accessibles à partir d'Internet.

Désactivation de l'édition Cyber Protect - Advanced/Standard

Les modifications suivantes auront une incidence sur le locataire sélectionné et ses locataires enfants qui disposaient de l'édition Cyber Protect - Advanced/Standard :

- L'édition Cyber Protect - Advanced/Standard deviendra indisponible.
- Tous les plans de protection seront révoqués, tous les appareils seront désinscrits et leurs sauvegardes seront supprimées.
- Toutes les fonctionnalités de Cyber Protect seront désactivées.

2.1.3 Changement de l'édition du service Cyber Protection pour les clients

Mise à niveau des éditions pour vos locataires clients

Pour mettre à niveau l'édition d'un locataire partenaire, accédez à **Clients** > **<particular_partner>** > onglet **Configurer** et changez d'édition. Cette mise à niveau de l'édition peut prendre jusqu'à 10 minutes.

Édition <actuelle> > Édition <cible>

Les modifications suivantes s'appliqueront au locataire sélectionné et à ses locataires enfants :

- Les fonctionnalités de l'édition <cible> deviendront disponibles.
- Tous les plans de protection qui utilisent les fonctionnalités de l'édition <actuelle> continueront de fonctionner.
- Tous les appareils enregistrés et leurs sauvegardes seront conservés.
- Les statistiques et les quotas d'utilisation seront migrés vers les éléments connexes de l'édition <cible> dans le portail de gestion et le rapport d'utilisation. Les statistiques d'utilisation historique seront conservées.

Rétrogradation des éditions pour vos locataires clients

La rétrogradation de l'édition peut prendre jusqu'à 10 minutes. Saisissez votre identifiant pour confirmer la rétrogradation de l'édition.

Advanced edition > Standard edition

Les modifications suivantes s'appliqueront au locataire sélectionné et à ses locataires enfants :

- Les fonctionnalités de l'édition Cyber Backup - Advanced deviendront indisponibles.
- Tous les plans de protection qui utilisent les fonctionnalités de l'édition Cyber Backup - Advanced cesseront de fonctionner.
- Tous les appareils enregistrés et leurs sauvegardes seront conservés.
- Les statistiques et les quotas d'utilisation seront migrés vers les éléments connexes de l'édition Cyber Backup Standard dans le portail de gestion et le rapport d'utilisation. Les statistiques d'utilisation historique seront conservées.

Disaster Recovery edition > Advanced/Standard edition

Les modifications suivantes s'appliqueront au locataire sélectionné et à ses locataires enfants :

- Les fonctionnalités de l'édition Cyber Backup Disaster Recovery deviendront indisponibles.
- Tous les plans de protection qui utilisent les fonctionnalités de l'édition Cyber Backup - Disaster Recovery cesseront de fonctionner.
- Tous les appareils enregistrés et leurs sauvegardes seront conservés.
- Tous les serveurs de restauration, les serveurs primaires et leurs sauvegardes seront conservés.
- Toutes les configurations réseau de reprise d'activité après sinistre seront conservées.
- Les appliances VPN resteront enregistrées.
- Les statistiques et les quotas d'utilisation seront migrés vers les éléments connexes de l'édition Cyber Backup Advanced/Standard dans le portail de gestion et le rapport d'utilisation. Les statistiques d'utilisation historique seront conservées.

Édition Cyber Protect > Édition Cyber Backup

Les modifications suivantes s'appliqueront au locataire sélectionné et à ses locataires enfants :

- Les fonctionnalités de l'édition Cyber Protect deviendront indisponibles.
- Le reste des changements sont décrits ci-dessus dans l'article, en fonction du changement d'édition réalisé.

2.1.4 Activer ou désactiver des éléments

Pour savoir comment activer ou désactiver les éléments pour un locataire, reportez-vous à la section « Création d'un locataire (p. 20) ».

La capacité de désactiver les éléments et le résultat de ces actions sont répertoriés 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 Office 365 et G Suite)	Peut être désactivé lorsque l'utilisation est égale à zéro.	La sauvegarde et la récupération des sources de données (y compris Office 365 et G Suite) 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 (p. 10) ».
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.

2.1.5 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.

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.

2.1.5.1 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**
- **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 Office 365**

  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**, des fichiers **OneDrive** ou les deux. Les administrateurs de l'entreprise peuvent afficher le quota et l'utilisation dans le portail de gestion, mais ne peuvent pas définir de quota pour un utilisateur.

- **Office 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. Si le quota est activé, un nombre illimité de sites SharePoint Online 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 SharePoint Online dans les rapports d'utilisation.

La sauvegarde de sites SharePoint Online n'est disponible que pour les clients qui disposent d'au moins un quota de postes Office 365 en plus. Ce quota est uniquement vérifié et ne sera pas utilisé.

- **Postes G Suite**

  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, mais ne peuvent pas définir de quota pour un utilisateur.

- **Drive partagé G Suite**

  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 G Suite. 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 G Suite n'est disponible que pour les clients qui disposent d'au moins un quota de postes G Suite en plus. Ce quota est uniquement vérifié et ne sera pas utilisé.

Un poste Office 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 G Suite 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**

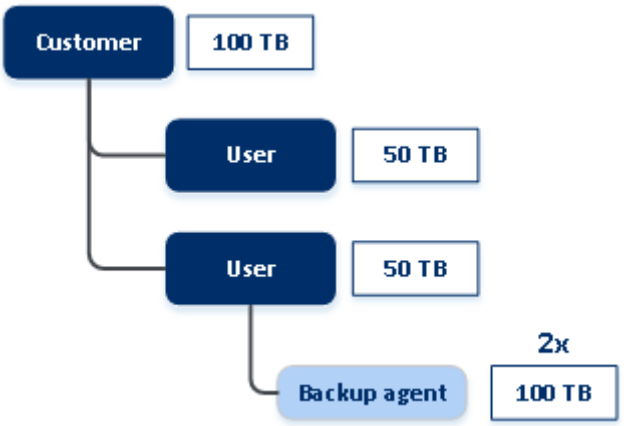
Le quota de **ressources Cloud** combine le quota de stockage de sauvegarde et le quota de reprise d'activité après sinistre. Le quota de stockage des sauvegardes limite la taille totale des sauvegardes situées dans le stockage dans le Cloud. Lorsque le dépassement de quota de stockage de sauvegarde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

Dépassement du quota dur pour le stockage de sauvegarde

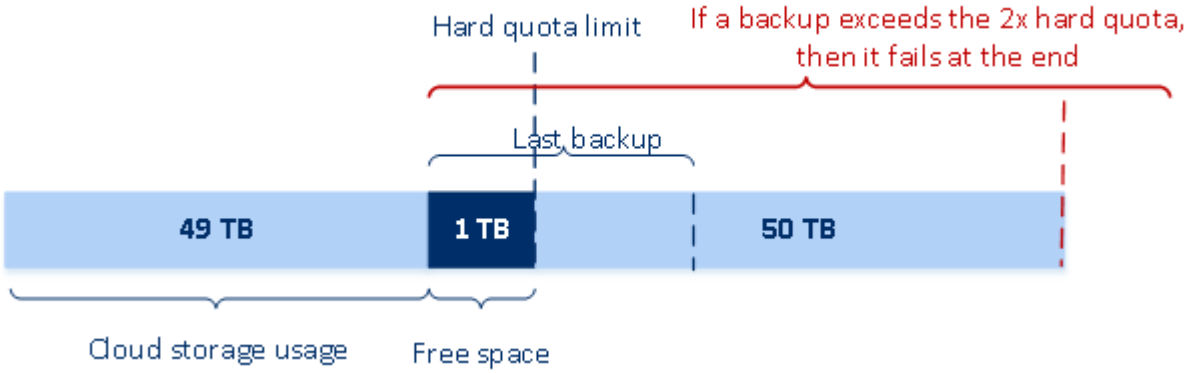
Concernant le stockage de sauvegarde, son quota dur peut être dépassé jusqu'à deux fois le quota dur défini. Le certificat de l'agent de protection possède deux fois le quota technique qui permet à un agent de dépasser le quota inconditionnel du client lorsqu'il n'est pas encore atteint lors d'une sauvegarde en cours d'exécution. La sauvegarde suivante ne sera pas possible si le quota du locataire est dépassé. Si la valeur multipliée par deux du quota (dans le certificat) est atteinte lors de la création de la sauvegarde, alors la sauvegarde échouera.

Exemple : Vous avez défini le quota dur du stockage dans le Cloud à 100 To pour un locataire client, ce qui signifie que la somme totale des quotas durs attribués aux locataires ne peut pas dépasser 100 To. Vous avez décidé de diviser le quota dur pour deux utilisateurs de façon égale. Cela signifie que, techniquement, chaque agent d'utilisateur possède 100 To de quota technique. Cependant, cela ne signifie pas que l'agent puisse sauvegarder des machines jusqu'à ce que la limite de 100 To soit

atteinte. Cela signifie simplement que si le quota dur est quasiment atteint au début de la création de la sauvegarde, alors la sauvegarde sera réalisée, à moins que sa taille ne soit trop importante, et que même le double du quota dur ne soit pas suffisant.



Dans le modèle ci-dessous, un utilisateur possède 1 To d'espace disponible, mais la taille de la sauvegarde est plus importante, pas exemple 3 To. Dans ce cas, la sauvegarde sera bien réalisée, même si la limite du quota dur de l'espace de stockage dans le Cloud est dépassée de 2 To. Si la taille de la sauvegarde était de 53 To, alors la création de la sauvegarde commencerait, mais échouerait lorsque la limite du stockage dans le Cloud (100 To) serait atteinte.



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.

2.1.5.2 Quotas de reprise d'activité après sinistre

Remarque *Les éléments de reprise d'activité après sinistre ne sont disponibles que dans les éditions Disaster Recovery.*

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**

  Ce stockage est utilisé par les serveurs primaires et de restauration. Si le quota est atteint, il n'est pas possible de créer des serveurs primaires et de restauration, ou d'ajouter/étendre des disques à des serveurs primaires existants. Si le quota est dépassé, il n'est 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.

2.1.5.3 Quotas pour la synchronisation et le partage de fichiers

Vous pouvez définir les quotas suivants pour la synchronisation et le partage de fichiers pour un locataire :

- **Utilisateurs**

  Le quota définit le nombre d'utilisateurs pouvant accéder à ce service.

- **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.

2.1.5.4 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.

2.1.5.5 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.

2.1.6 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	Stations de travail	Machines virtuelles	Postes Office 365	Postes G Suite	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 Office 365				+				
Agent pour G Suite					+			
Programme d'installation complet pour Windows	+	+	+				+	+
Mobile (iOS et Android)						+		

2.2 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.

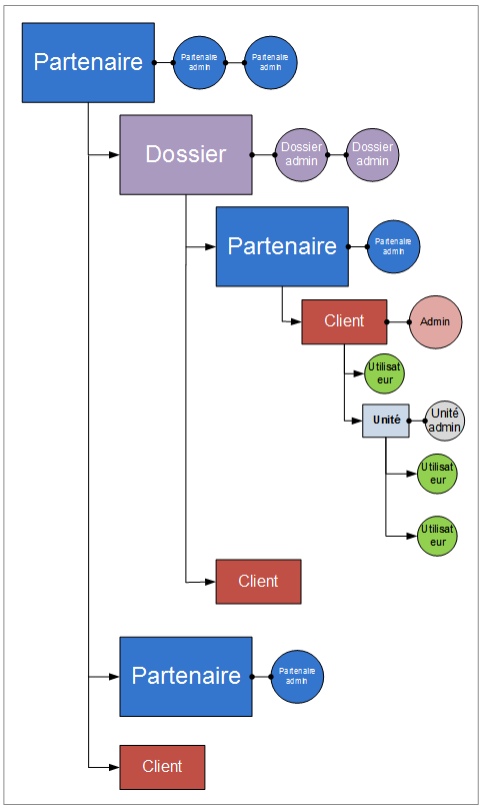
Chaque compte fait partie d'un locataire. Un locataire est une partie des ressources (tel que des comptes utilisateur et des locataires enfants) et des offres de service (les services et éléments activés en son sein) d'un portail de gestion, dédiée à un partenaire ou à un client. La hiérarchie établie 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.

Les administrateurs de niveau client ou supérieur peuvent limiter l'accès des administrateurs de niveau supérieur à leur locataire (p. 62).

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



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

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.

2.3 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
- Windows Internet Explorer 11 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.

3 Utilisation du portail de gestion

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

3.1 Activation du compte administrateur

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

- **Un lien d'activation du compte**. Cliquez sur le lien et configurez le mot de passe du compte administrateur. Conservez l'identifiant présent sur la page d'activation du compte.
- **Un lien vers la page de connexion**. L'identifiant et le mot de passe sont les mêmes que pour l'étape précédente.

3.2 Accès au portail de gestion

1. Allez sur la page de connexion au service. L'adresse de la page de connexion apparaît dans le courrier électronique d'activation.

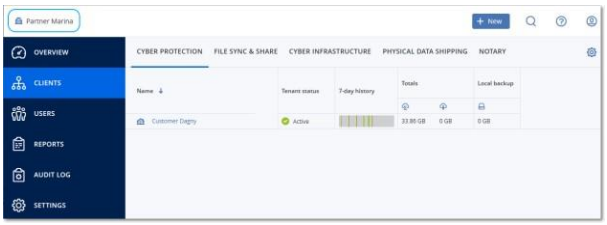
2. Saisissez l'identifiant, puis cliquez sur **Suivant**.
3. Saisissez le mot de passe, puis cliquez sur **Suivant**.
4. Cliquez sur **Portail de gestion**.

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

3.3 Navigation dans le portail de gestion

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

Le niveau de hiérarchie le plus haut possible est sélectionné par défaut. Cliquez sur le nom du locataire 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 **Utilisateurs** affiche uniquement les comptes client existant dans le locataire 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.

3.4 Accès aux services

Onglet Vue d'ensemble

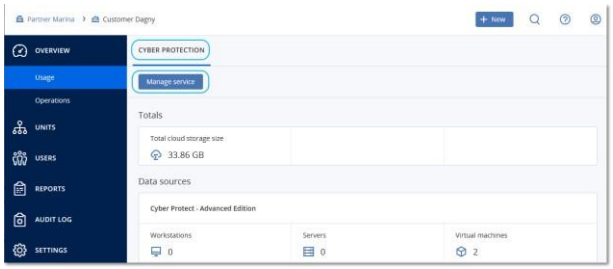
La section **Vue d'ensemble** > **Utilisation** fournit une présentation de l'utilisation du service et vous permet d'accéder aux services au sein du locataire dans lequel vous travaillez.

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

1. Naviguez vers le locataire (p. 19) 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.

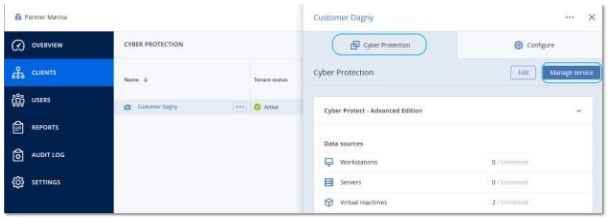


Onglet Clients

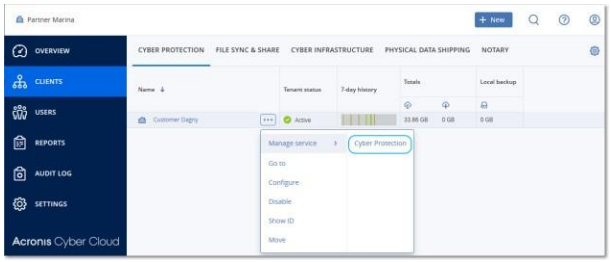
L'onglet **Clients** affiche les locataires enfants du locataire dans lequel vous travaillez et vous permet d'accéder aux services de ce locataire.

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.

3.5 Création d'un locataire

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.

Il se peut que vous souhaitiez créer un nouveau locataire **unité** dans un locataire client existant lorsque vous étendez le service à une nouvelle unité d'organisation.

Pour créer un locataire

1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire (p. 19) dans lequel vous souhaitez créer un locataire.
3. Dans le coin supérieur droit, cliquez sur **Nouveau**, puis cliquez sur l'un des éléments suivants, selon le type de locataire que vous souhaitez créer :
   - **Client**
   - **Partenaire**
   - **Dossier**
   - **Utilisateur**

   Les types disponibles dépendent du type de locataire parent.
4. Dans la section **Nom**, indiquez le nom du nouveau locataire.
5. [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, ce dernier sera totalement 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 locataire a utilisé le mode d'évaluation pendant un mois complet, le mode de celui-ci passe automatiquement en mode production.*
6. [Facultatif] Dans **Langue**, changez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée au sein de ce locataire.
7. 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. Le locataire n'aura d'administrateur que lorsque vous en aurez créé un.
   - Pour configurer les services pour le locataire et créer un administrateur de locataire, cliquez sur **Suivant**.
8. [Facultatif, non applicable à un locataire unité] Désactivez les commutateurs correspondant aux services que vous souhaitez désactiver pour le locataire. Les services désactivés seront cachés aux utilisateurs au sein du locataire et de ses locataires enfants.

   [Si vous créez un partenaire] Pour le service Cyber Protection, sélectionnez les éditions qui seront disponibles.

   [Si vous créez un client] Pour le service Cyber Protection, sélectionnez l'une des éditions qui sera disponible.

   Cliquez sur **Suivant** quand tout est prêt.
9. [Facultatif, non applicable à un locataire unité] Configurer les éléments pour le locataire :
   a. Au sein de chaque 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.
   b. 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 la section « Gérer les emplacements et le stockage » (p. 38).

c. 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.

d. [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.

10. Effectuez l'une des actions suivantes :
    - Pour créer un administrateur de locataire, cliquez sur **Suivant**, puis suivez les étapes décrites dans « Création d'un compte utilisateur » (p. 23) à partir de l'étape 4. Si vous changez d'avis, vous pouvez cliquer sur **Ignorer et fermer** pour annuler la création d'un administrateur.
    - Pour créer un locataire sans administrateur, cliquez sur **Enregistrer et fermer**. Vous pourrez ajouter des administrateurs au locataire ultérieurement.

Le locataire nouvellement créé s'affiche dans l'onglet **Clients**.

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

3.6 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 Axproo Cyber Cloud.
- 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**.

3.7 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 » (p. 22).

Important *La suppression d'un locataire est irréversible !*

Pour supprimer un client

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le client 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.

3.8 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/unité — pour déléguer la gestion du service à d’autres personnes dont les droits d’accès seront strictement limités au client/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.

Veuillez noter que les comptes existants ne peuvent pas être déplacés entre les locataires. 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 (p. 19) dans lequel vous souhaitez créer un compte utilisateur.
3. Dans le coin supérieur droit, cliquez sur **Nouveau** > **Utilisateur**.
4. Indiquez les informations de contact suivantes relatives au compte :
   - **Adresse e-mail**

- [Facultatif]**Prénom**
- [Facultatif]**Nom**
- [Facultatif] Pour indiquer un identifiant différent de l'adresse e-mail indiquée, décochez la case **Utiliser l'adresse e-mail en tant qu'identifiant**, puis indiquez l'identifiant.

  Important *Chaque compte doit disposer d'un identifiant unique.*

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

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 **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.

3.9 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**.

3.10 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 » (p. 24).

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.

3.11 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.

3.12 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 (p. 29) 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://itunes.apple.com/sg/app/google-authenticator/id388497605?mt=8)

     Version Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_SG)
   - Microsoft Authenticator

     Version de l'application iOS (https://app.adjust.com/n094ls?campaign=appstore_ios&fallback=https://itunes.apple.com/app/microsoft-authenticator/id983156458)

     Version Android (https://app.adjust.com/n094ls?campaign=appstore_android&fallback=https://play.google.com/store/apps/details?id=com.azure.authenticator)

   Important *Les utilisateurs doivent s'assurer que l'heure indiquée sur l'appareil 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.

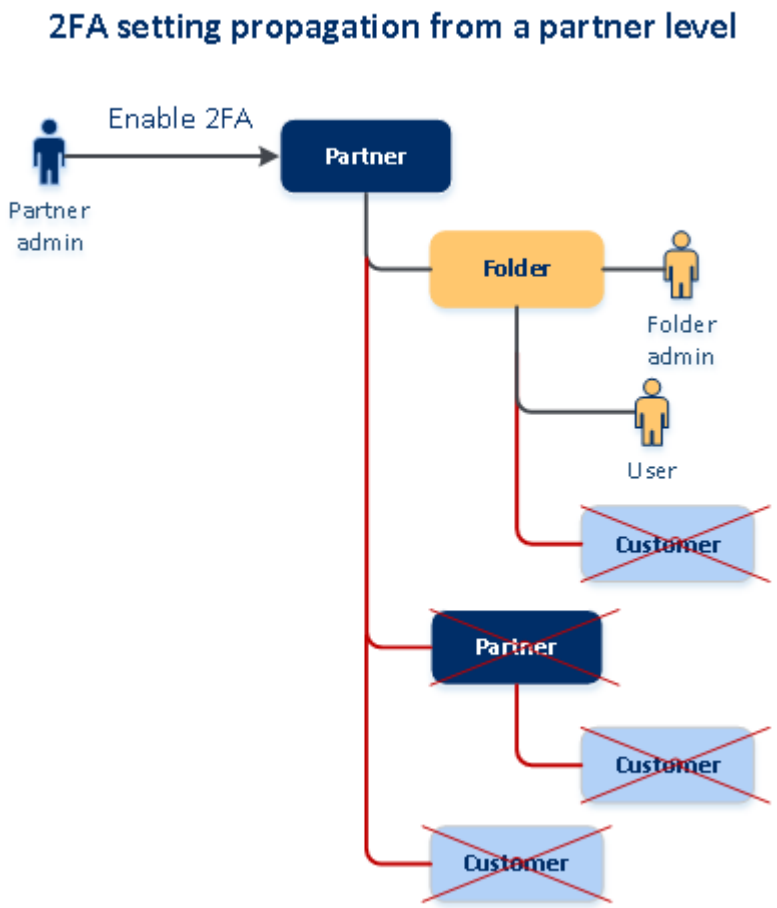
3.12.1 Propagation de la configuration de l'authentification à deux facteurs à tous les niveaux de locataires

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

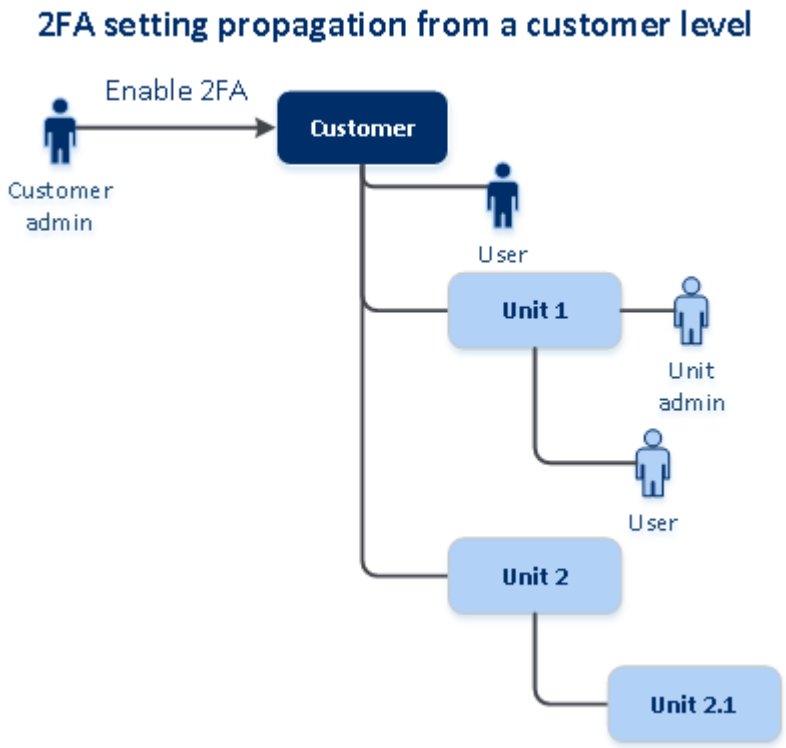
- Pour votre propre organisation.
- Pour votre locataire enfant (uniquement si l'option **Accès à l'assistance** est activée au sein de ce locataire enfant).

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.

3.12.2 Configurer l'authentification à deux facteurs pour votre locataire

Pour activer l'authentification à deux facteurs pour votre locataire

1. Dans le portail de gestion, accédez à **Paramètres** > **Sécurité**.
2. Pour activer l'authentification à deux facteurs, faites glisser le curseur. Pour confirmer, cliquez sur **Activer**.

La barre de progression affiche le nombre d'utilisateurs ayant configuré l'authentification à deux facteurs pour leurs comptes. En conséquence, l'authentification à deux facteurs est activée pour votre organisation. Aucun utilisateur de l'organisation ne pourra se connecter jusqu'à ce qu'il ait configuré l'authentification à deux facteurs dans son compte. Après ça, les utilisateurs seront invités à saisir leur identifiant et leur mot de passe, ainsi que le code TOTP pour se connecter au système.

Dans l'onglet **Utilisateurs**, la colonne de **statut 2FA** apparaît. Vous pouvez suivre les utilisateurs qui configuré l'authentification à deux facteurs pour leur compte.

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, faites glisser le curseur. Pour confirmer, 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 l'onglet **Utilisateurs**, la colonne de **statut 2FA** est masquée.

3.12.3 Gestion de la configuration de l'authentification à deux facteurs pour les utilisateurs

Vous pouvez surveiller les paramètres d'authentification à deux facteurs de tous vos utilisateurs et réinitialiser les paramètres dans l'onglet **Utilisateur** du portail de gestion.

Surveillance

Dans le portail de gestion, sous l'onglet **Utilisateurs**, vous pouvez voir une liste de tous les utilisateurs de votre organisation. Le **statut 2FA** se reflète 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, sous l'onglet **Utilisateurs**, trouvez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
2. Cliquez sur **Réinitialiser l'authentification à deux facteurs**.
3. 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, sous l'onglet **Utilisateurs**, trouvez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
2. Cliquez sur **Réinitialiser tous les navigateurs fiables**.
3. 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

Vous pouvez désactiver l'authentification à deux facteurs pour un utilisateur, mais la laisser activée pour les autres. Cela peut s'avérer nécessaire si l'utilisateur est utilisé pour accéder à l'API.

Important *Ne remplacez pas les utilisateurs normaux par des utilisateurs du service dans le but de désactiver l'authentification à deux facteurs, car il se pourrait que les utilisateurs ne puissent plus se connecter.*

1. Dans le portail de gestion, sous l'onglet **Utilisateurs**, trouvez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
2. Cliquez sur **Marquer comme compte de service**. En conséquence, un utilisateur reçoit un statut spécial d'authentification à deux facteurs, appelé **Compte de service.**
3. [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, sous l'onglet **Utilisateurs**, trouvez un utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur l'icône en forme de points de suspension.
2. 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.

3.12.4 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 (p. 30).

3.12.5 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.

3.13 Configuration de scénarios de vente additionnelle pour vos clients

La vente additionnelle consiste à persuader un client d'acheter quelque chose en plus ou quelque chose de plus onéreux.

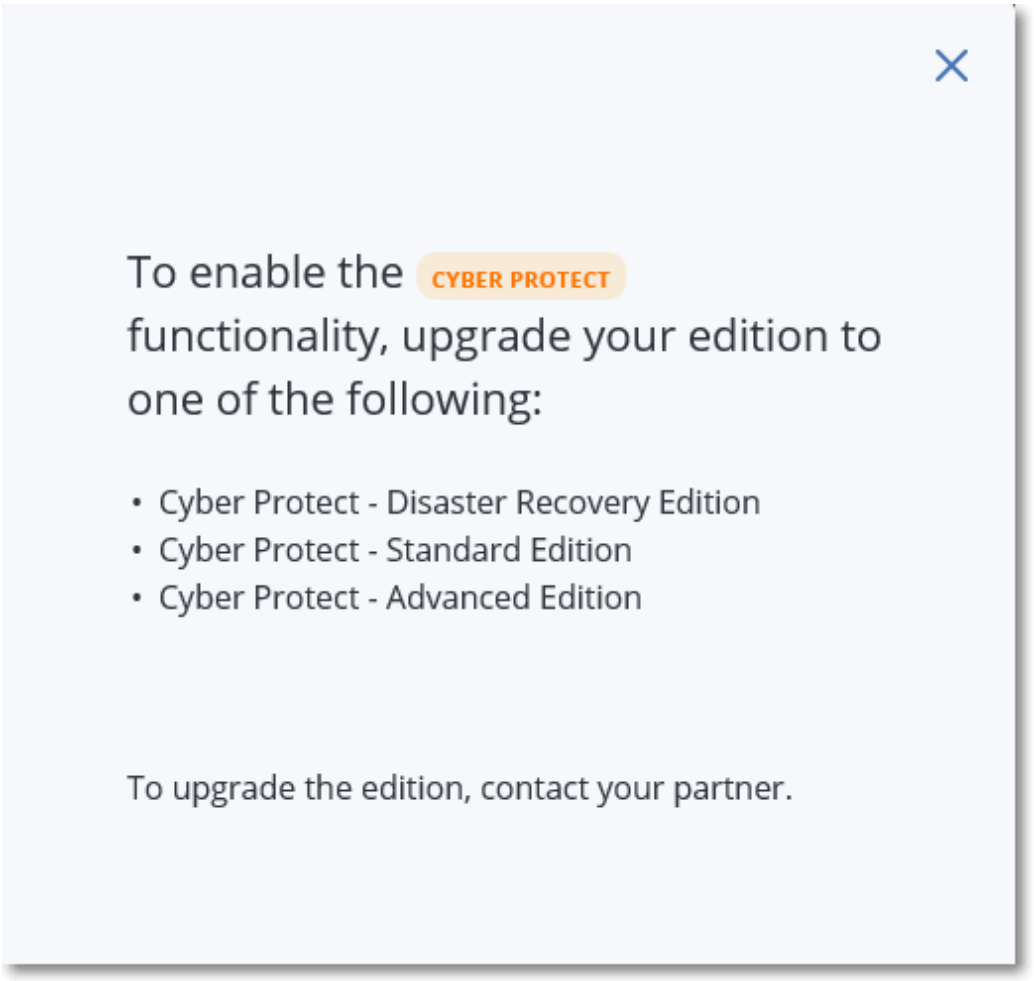
Cyber Protection possède six éditions différentes, dont les fonctionnalités et le prix varient. Nous vous invitons à promouvoir des éditions plus onéreuses et proposant des capacités plus avancées auprès des clients qui utilisent déjà une édition de base.

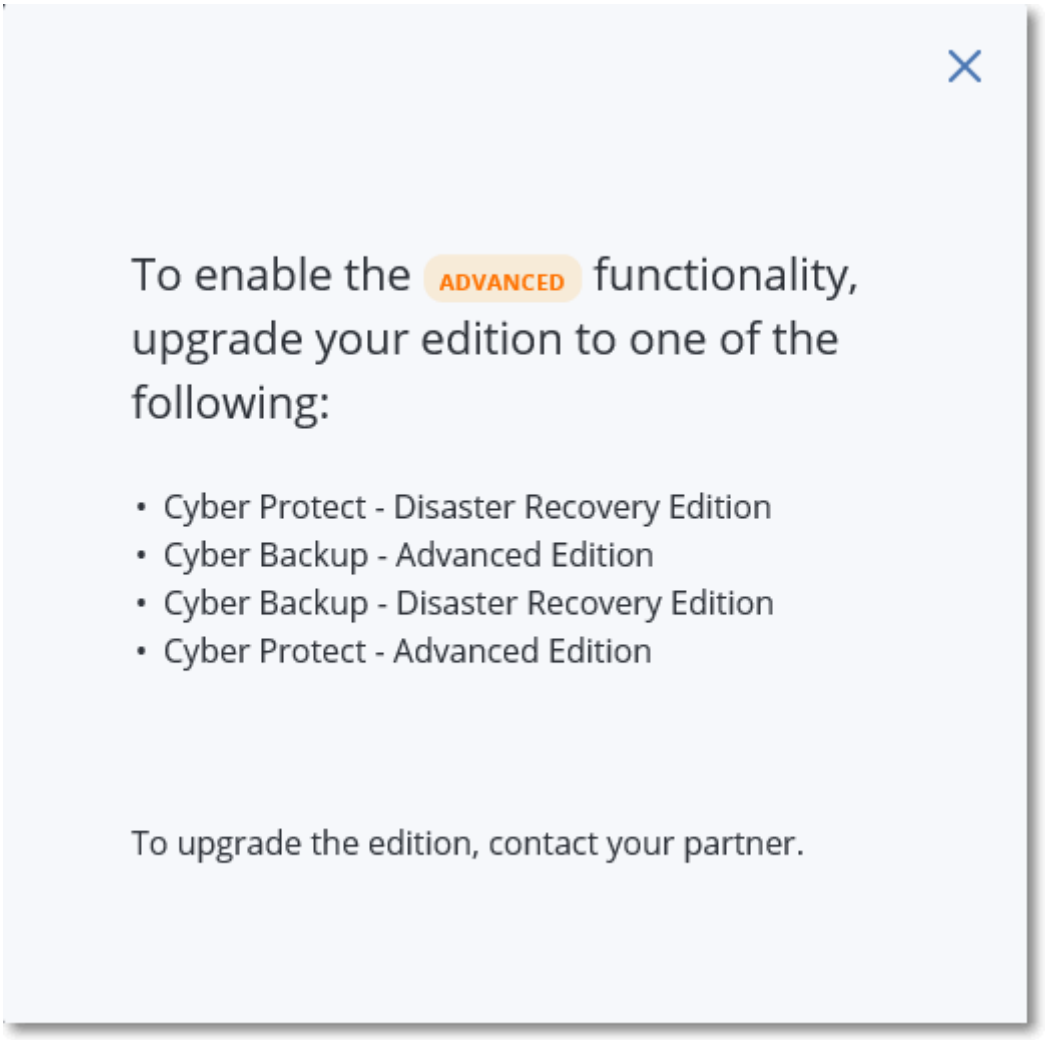
Vous pouvez activer ou désactiver la capacité de vente additionnelle par client. Par défaut, l'option de vente additionnelle est activée. Si vous activez la vente additionnelle pour un client, celui-ci verra des fonctionnalités supplémentaires qui ne seront pas disponibles tant qu'il n'aura pas acheté 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.





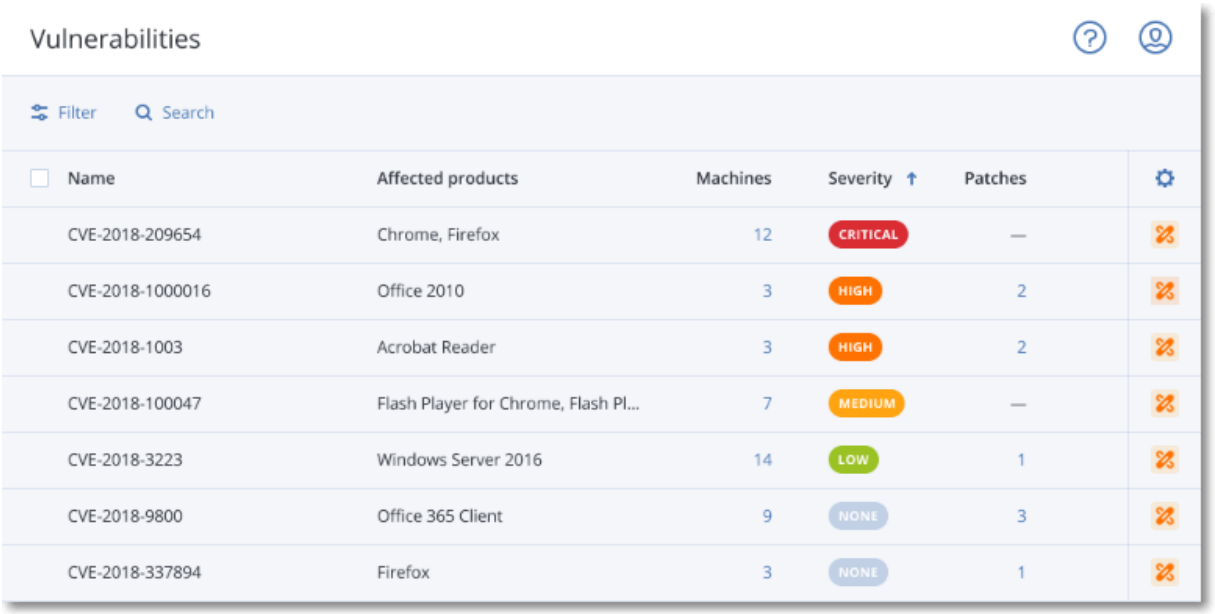
Pour activer ou désactiver la capacité de vente additionnelle pour un client.

1. Dans le portail de gestion, accédez à **Clients**.
2. Sélectionnez le client, accédez au volet de gauche, puis passez à 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

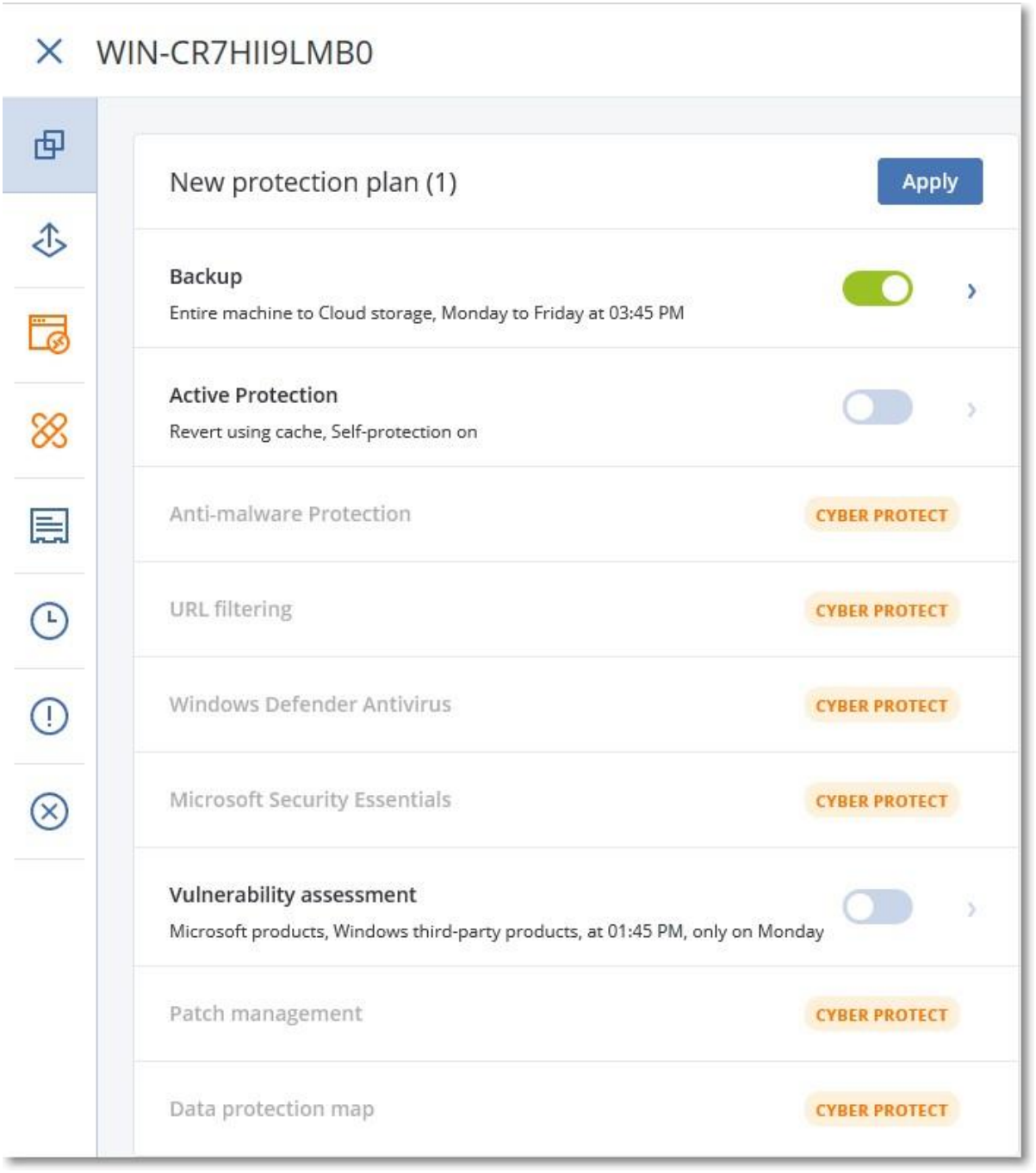
Liste des vulnérabilités

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.



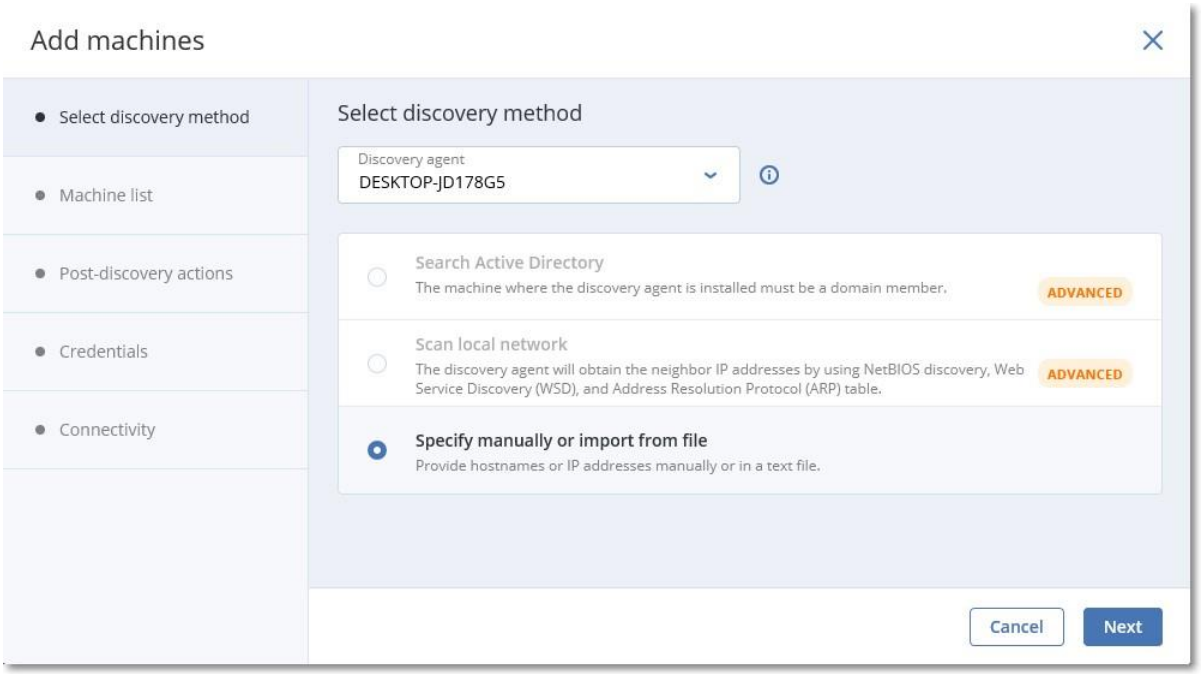
Créer ou modifier un plan de protection

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.

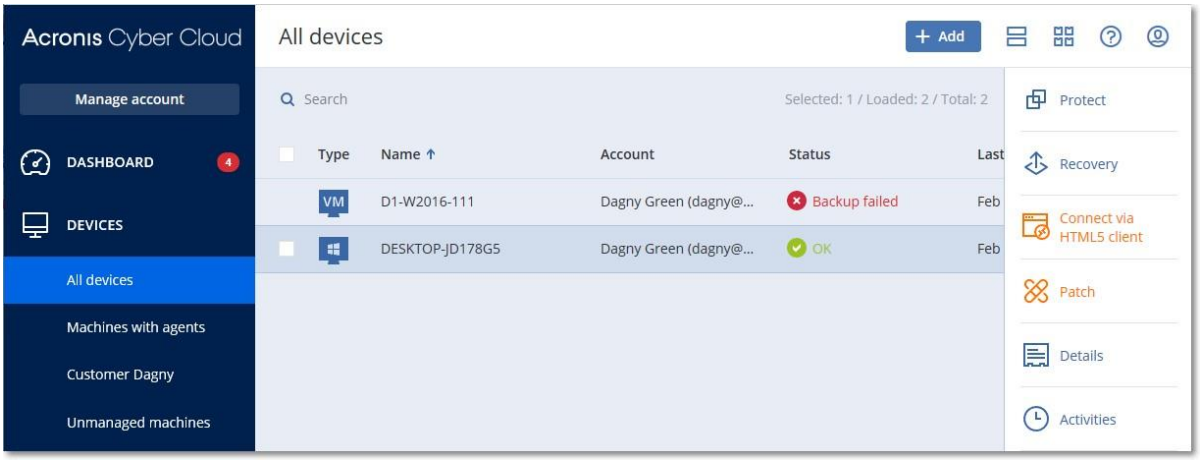


Actions dans la liste des périphériques.

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.



3.14 Gérer les emplacements et le stockage

La section **Paramètres** > **Emplacements** affiche les stockages 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 » (p. 39).

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

Lors de la création d'un locataire partenaire/dossier (p. 20), 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 (p. 20), 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.

3.14.1 Gestion du stockage

Ajouter de nouveaux stockages

- Service **Cyber Protection** :
  - Par défaut, les stockages de sauvegarde se trouvent dans les centres de données Axproo.
  - Si l'élément de **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 Axproo. 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 le support technique de Axproo sur https://www.Axproo.fr/support.
- Pour des informations concernant l'ajout de stockages qui seront utilisés par d'autres services, contactez le support technique de Axproo sur https://www.Axproo.fr/support.

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 (p. 19) 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.

3.15 Configuration de la marque

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 Axproo ou 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.

La fonctionnalité de configuration de la marque pour tous les services sera disponible dans les versions à venir. Certains services fournissent des fonctionnalités de marquage séparées. Pour

obtenir davantage d'informations, veuillez consulter les guides de l'utilisateur, disponibles dans les consoles de service.

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**. Le logo est également affiché dans le portail de gestion et les services. Cliquez sur le logo pour télécharger un fichier image.
- **Modèle de couleurs**. Le modèle de couleurs définit la combinaison de couleurs utilisée pour tous les éléments de l'interface utilisateur. Cliquez sur le modèle, puis choisissez un des modèles prédéfinis correspondant le plus à vos besoins.

  Astuce *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****.*

- **Agent Cyber Protection à marque blanche**. Cette option vous permet de définir tous vos partenaires et clients enfants si l'agent Cyber Protection (pour Windows, MacOS et Linux) et le moniteur Cyber Protection (pour Windows, MacOS et Linux) seront de marque Axproo ou à marque blanche. Si vous activez cette option, l'agent et le contrôle de la zone de notification seront à marque blanche. Cette option affecte les noms et les logos utilisés dans l'installateur et le moniteur Cyber Protection.

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 le coin 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 le coin supérieur droit de l'interface utilisateur du portail de gestion, puis sur **Aide**.

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.
- **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 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.

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 (p. 32) ».

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

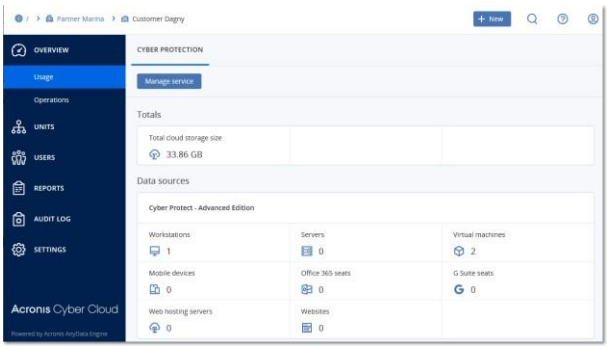
1. Connectez-vous au portail de gestion.
2. Naviguez vers le locataire (p. 19) dans lequel vous souhaitez configurer le marquage.
3. Cliquez sur **Paramètres** > **Marque**.
4. Cliquez sur **Permettre le marquage**.
5. Effectuez l'une des actions suivantes :
   - Configurez les éléments de marquage décrits ci-dessus.
   - 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**.
   - Cliquez sur **Restaurer les paramètres par Défaut** pour réinitialiser tous les éléments de marquage à leurs valeurs par défaut.

3.16 Surveillance

Pour accéder aux informations relatives à l'utilisation du service et aux opérations, cliquez sur **Vue d'ensemble**.

3.16.1 Utilisation

L'onglet **Uitlisation** 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.



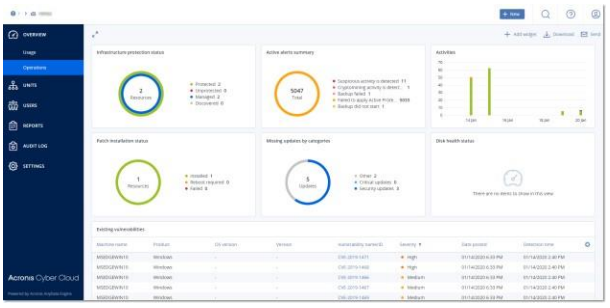
3.16.2 Opérations

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 (p. 19). 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 (p. 62), 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 locataires 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.

3.16.2.1 État de protection

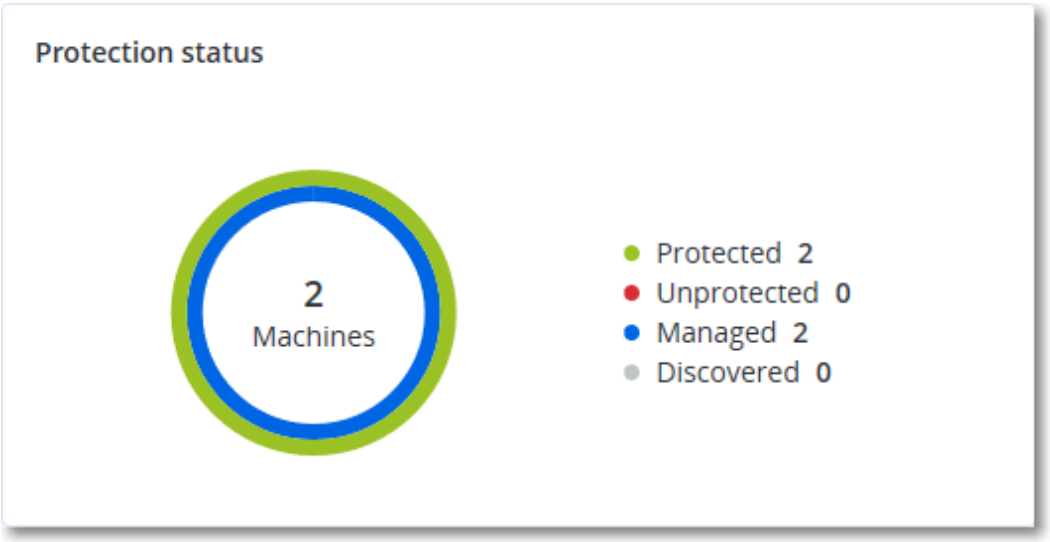
État de protection

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

Une machine peut présenter l'un des états suivants :

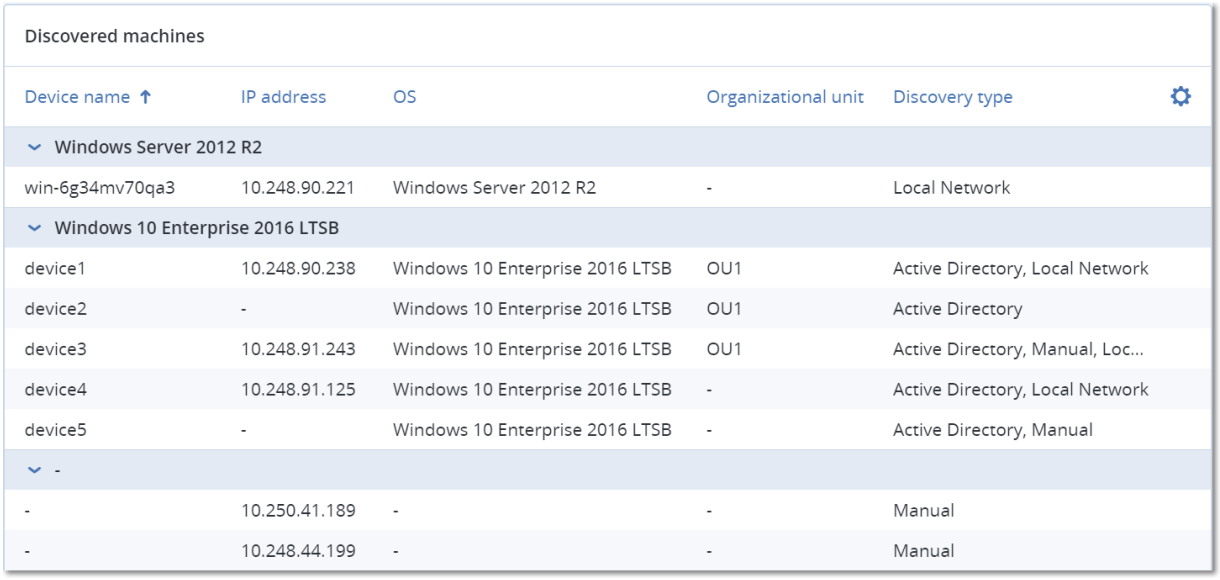
- **Protégé :** les machines sur lesquelles l'agent de protection est installé et un plan de protection est appliqué.
- **Non protégé :** les machines sur lesquelles l'agent de protection est installé, mais le plan de protection n'est pas appliqué.
- **Géré :** les machines sur lesquelles l'agent de 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

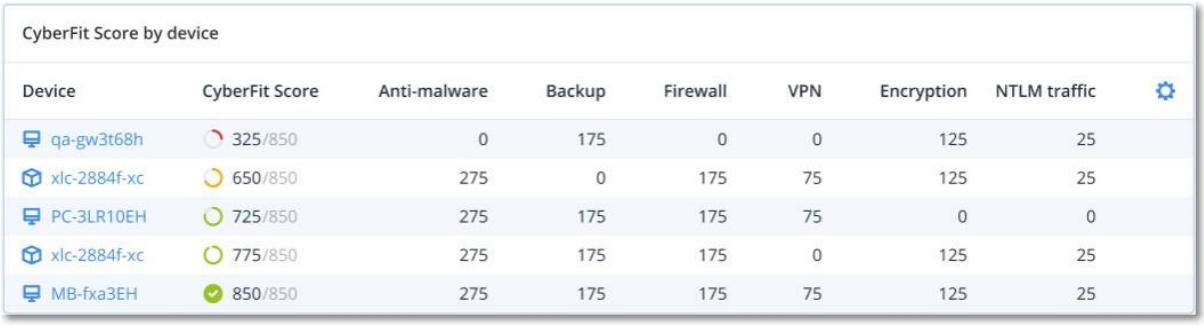
Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 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

3.16.2.2 Score CyberFit par machine

Ce widget affiche, pour chaque périphérique, le Score CyberFit total ainsi qu'une combinaison de ses scores :

- Protection contre les malware
- Sauvegarde
- Pare-feu
- VPN
- Chiffrement
- Trafic NTLM

Pour en savoir plus sur le Score CyberFit, reportez-vous à « Score CyberFit pour les machines (https://dl.managed-protection.com/u/baas/help/9.0/user/en-US/index.html#47837.html) ».



CyberFit Score by device

Device	CyberFit Score	Anti-malware	Backup	Firewall	VPN	Encryption	NTLM traffic
qa-gw3t68h	325/850	0	175	0	0	125	25
xlc-2884f-xc	650/850	275	0	175	75	125	25
PC-3LR10EH	725/850	275	175	175	75	0	0
xlc-2884f-xc	775/850	275	175	175	0	125	25
MB-fxa3EH	850/850	275	175	175	75	125	25

3.16.2.3 Prévision de l'état de santé du disque

La fonctionnalité de contrôle de l'état de santé du disque vous permet de suivre l'état de santé actuel du disque et d'obtenir une prévision de la santé du disque. Ces informations vous aident à éviter les problèmes de pertes de données suite à un plantage de disque. Les disques durs, tout comme les SSD, sont pris en charge.

Limites :
1. La prévision de l'état de santé du disque n'est prise en charge que pour les machines Windows.
2. Seuls les disques des machines physiques peuvent être surveillés. Les disques des machines virtuelles ne peuvent pas être surveillés ni être affichés dans le widget.

L'état de santé du disque peut présenter l'un des états suivants :

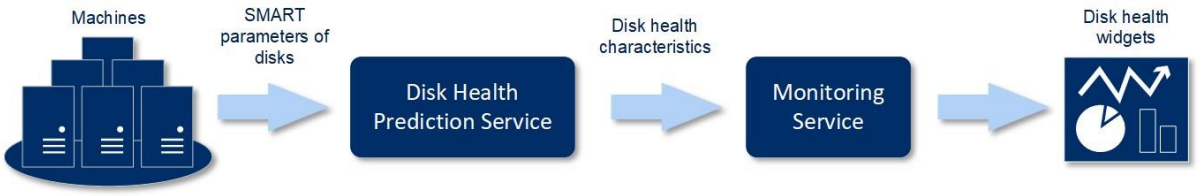
- **OK :** l'état de santé du disque est compris entre 70 et 100 %.
- **Avertissement :** l'état de santé du disque est compris entre 30 et 70 %.
- **Critique :** l'état de santé du disque est compris entre 0 et 30 %.
- **Calcul des données du disque :** l'état et la prévision de l'état de santé actuel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

Fonctionnement

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

1. L'agent collecte les paramètres SMART des disques et transmet ces données au service Prévision de l'état de santé 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'état de santé du disque traite les paramètres SMART, effectue des prévisions, et fournit les caractéristiques d'état de santé 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 toujours d'un mois.
3. Le service de surveillance obtient les caractéristiques de l'état de santé du disque et se sert de ces données dans des widgets d'état de santé du disque, qui s'affichent pour les utilisateurs dans la console.

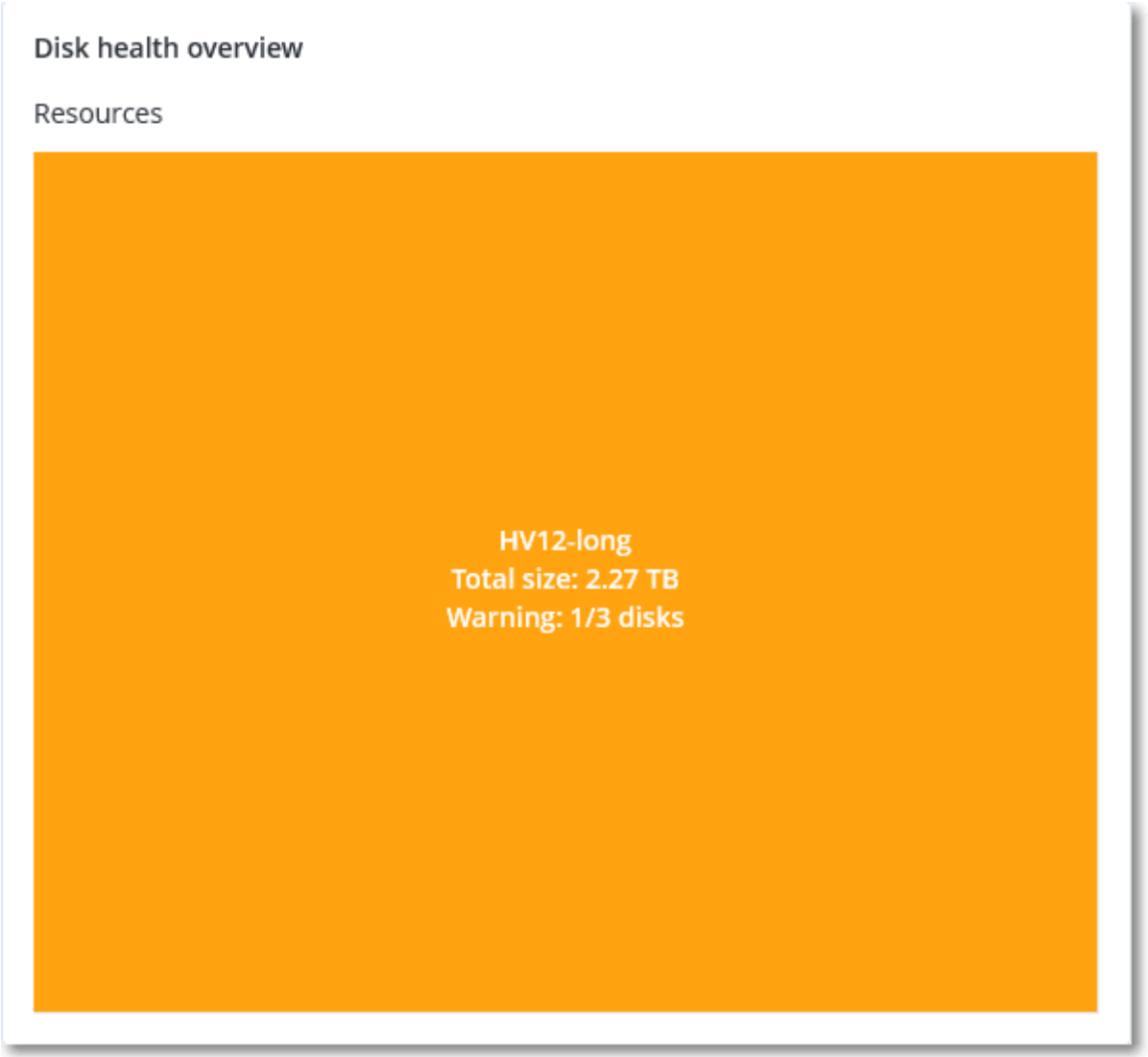


Widgets de l'état de santé du disque

Les résultats de la surveillance de l'état de santé du disque sont disponibles dans le tableau de bord, dans les widgets liés à l'état de santé du disque :

- **Vue d'ensemble de l'état de santé du disque :** un widget sous forme de carte proportionnelle, qui possède trois niveaux de détail que vous pouvez explorer tour à tour :
  - Niveau locataire client : affiche des informations résumées concernant l'état du disque en fonction des clients que vous avez sélectionnés. Le widget représente les données d'état du disque les plus critiques. Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur de votre souris sur un bloc particulier. La taille de bloc d'un client dépend de la taille totale de l'ensemble de ses disques. La couleur du bloc d'un client dépend de l'état de disque le plus critique identifié.

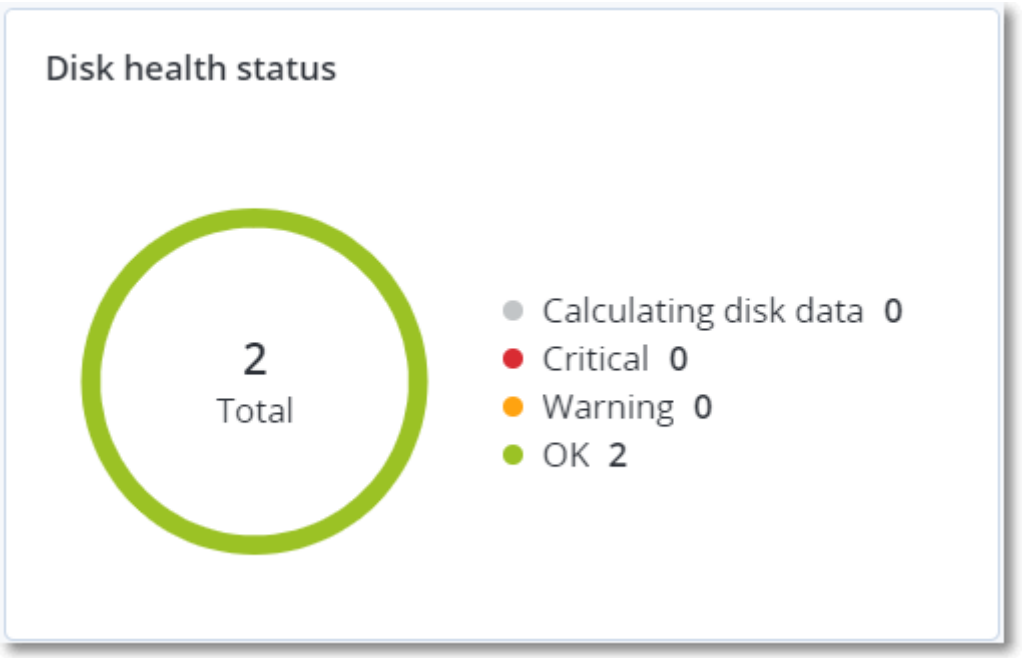
- Niveau machine : affiche des informations résumées concernant l'état du disque en fonction des machines client que vous avez sélectionnées. Le widget représente les données d'état du disque les plus critiques. Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur de votre souris sur un bloc particulier. La taille du bloc d'une machine 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'état actuel de tous les disques pour le client et la machine sélectionnés. Chaque bloc de disque présente une prévision du changement de l'état du disque :
  - Sera altéré (probabilité de prévision de l'état de santé du disque en pourcentage)
  - Restera stable (probabilité de prévision de l'état de santé du disque en pourcentage).

- Sera amélioré (probabilité de prévision de l'état de santé du disque en pourcentage).

- **État de santé du disque :** un widget sous forme de diagramme circulaire, montrant le nombre de disques pour chaque état.



3.16.2.4 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.

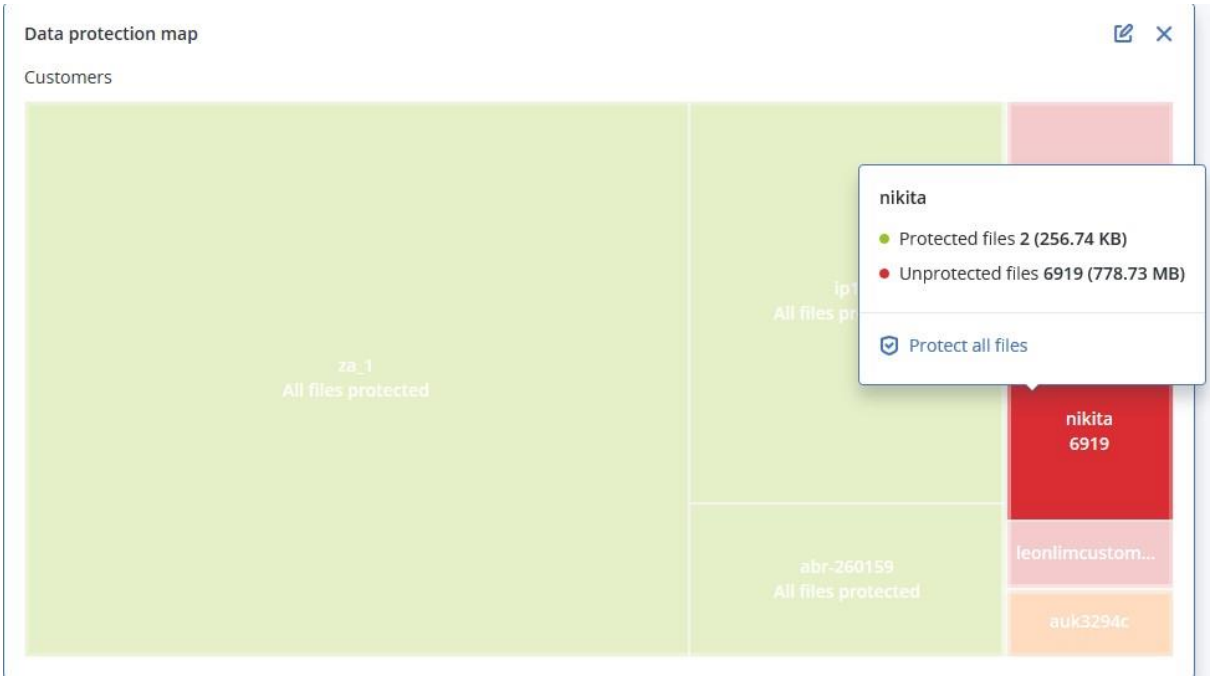
La taille de chaque bloc dépend du nombre total ou de la taille totale des fichiers importants qui appartiennent à un client ou à une machine.

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

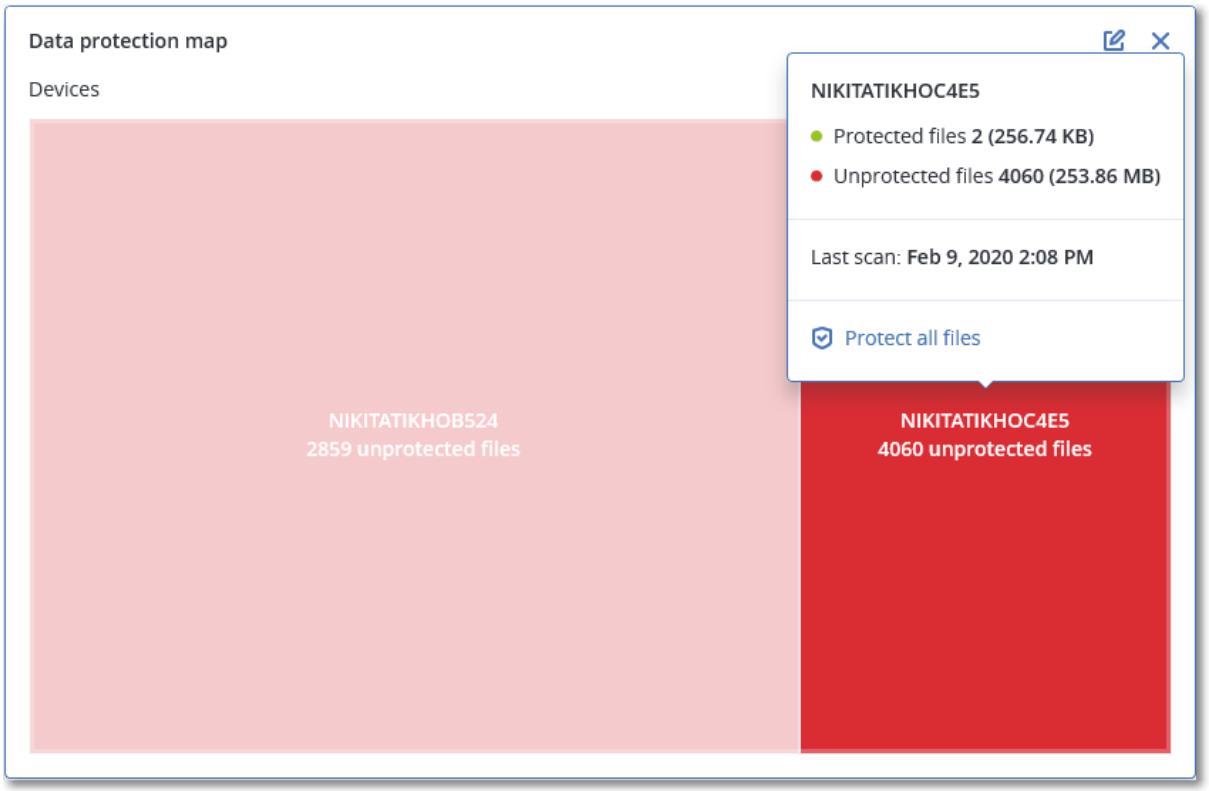
- **Critique :** de 51 à 100 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés pour le locataire, la machine ou l'emplacement client sélectionné.
- **Faible :** de 21 à 50 % des fichiers non protégés et présentant l'extension que vous avez spécifiée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

3.16.2.5 Widgets d'évaluation des vulnérabilités

Ordinateurs 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 :

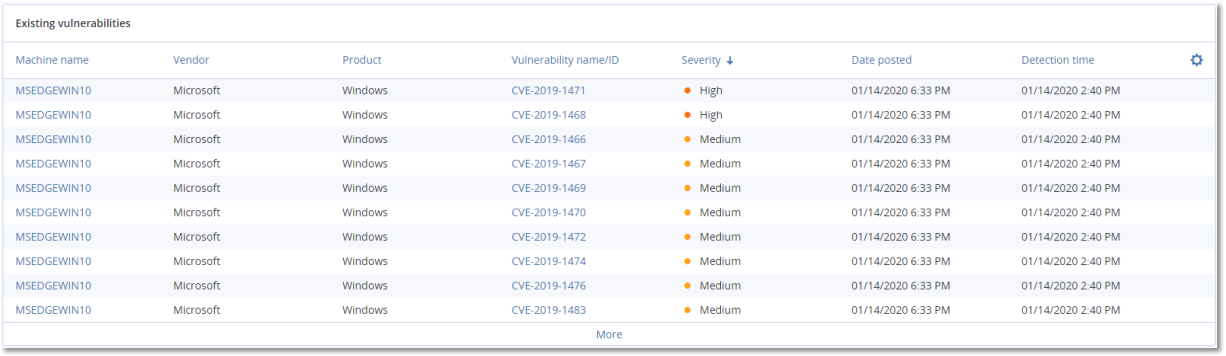
- Sécurisé : aucune vulnérabilité n'a été trouvée
- Critique : 9,0 – 10,0 CVSS
- Élevé : 7,0 – 8,9 CVSS
- Moyen : 4,0 – 6,9 CVSS
- Faible : 0,1 – 3,9 CVSS

- 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 :

- **Heure de détection** : date et heure à laquelle une vulnérabilité a initialement été détectée sur une machine.
- **Date de publication** : 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	Date posted	Detection time
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1471	High	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1468	High	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1466	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1467	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1469	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1470	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1472	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1474	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1476	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1483	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM

More

3.16.2.6 Widgets d'installation des correctifs

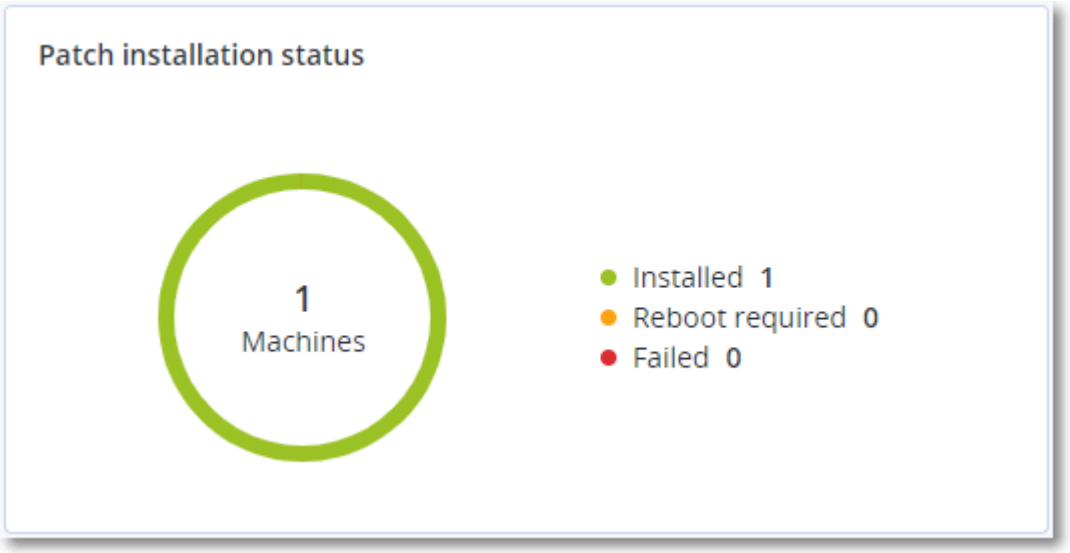
Il existe quatre widgets en lien avec la fonctionnalité de gestion des correctifs.

Statut d'installation des correctifs

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

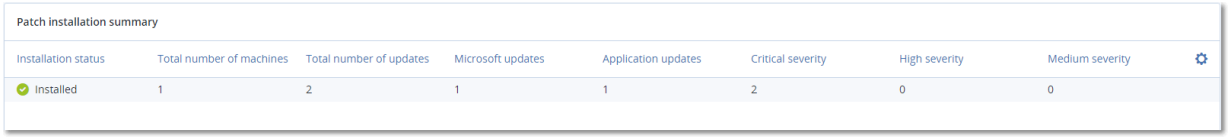
- **Installé :** tous les correctifs disponibles sont installés sur une machine.
- **Redémarrage nécessaire :** après l'installation des correctifs, un redémarrage est requis pour une machine.

- **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.



Historique d'installation des correctifs

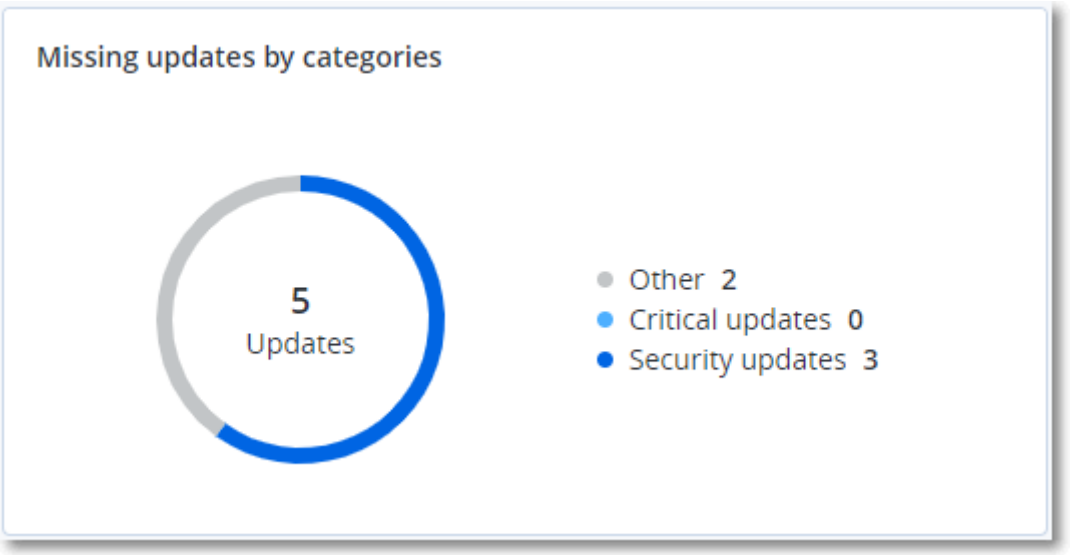
Ce widget affiche des informations détaillées au sujet des correctifs sur les machines.

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 :

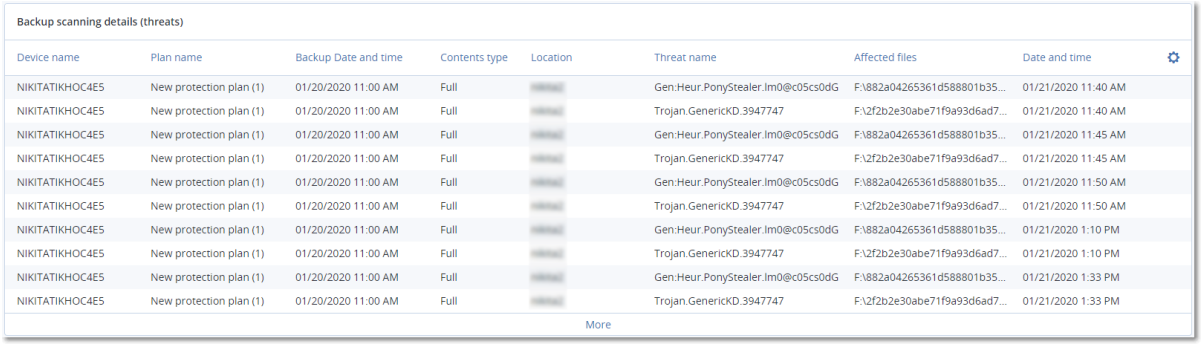
- Mises à jour de sécurité
- Mises à jour critiques

- Autre



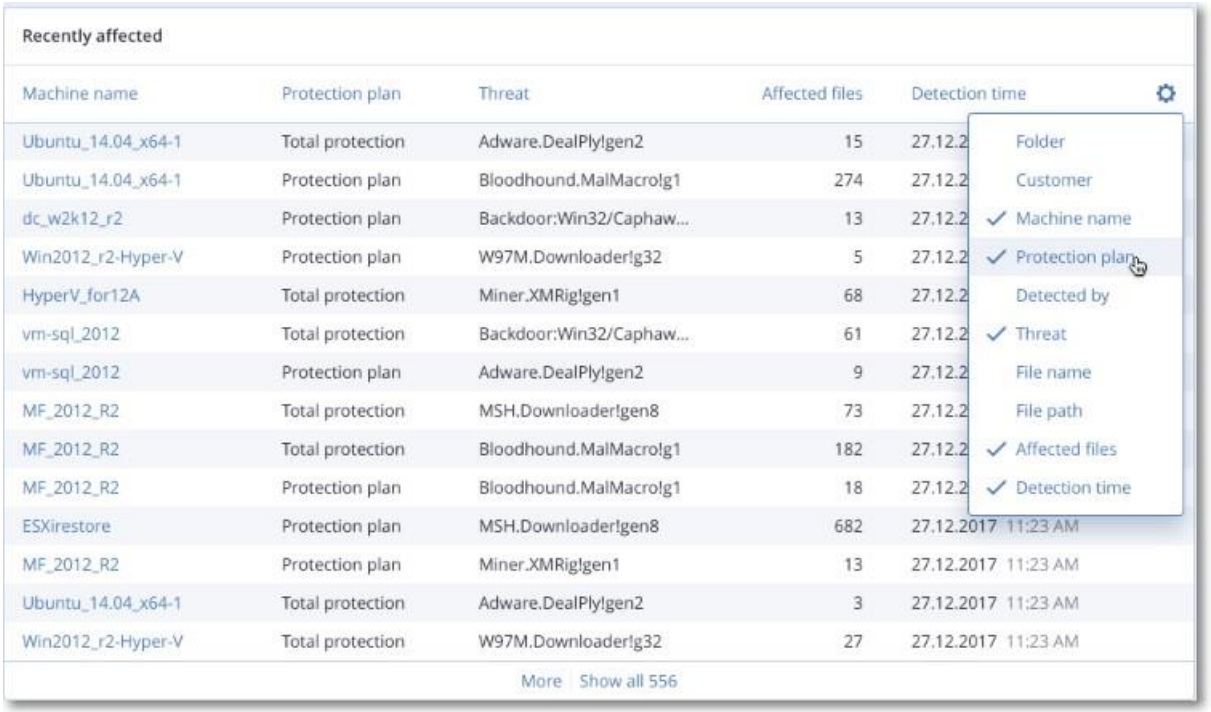
3.16.2.7 Détails de l'analyse de la sauvegarde

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



3.16.2.8 Affectés récemment

Ce widget affiche des informations détaillées au sujet des machines récemment infectées. Vous y trouverez des informations concernant les menaces détectées et le nombre de fichiers infectés.



3.17 Rapports

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

3.17.1 Utilisation

Les rapports d'utilisation fournissent des données historiques sur l'utilisation des services.

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 mesures 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 mesures 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, partenaires et utilisateurs**

  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.

Rapports 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 comme décrit ci-dessus.

Rapports 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 (p. 19) 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**

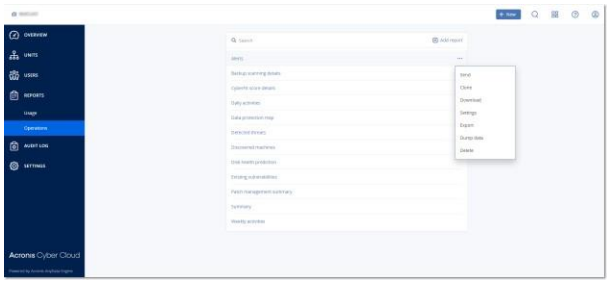
- **Personnalisée**

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. Pour générer le rapport, cliquez sur **Générer et envoyer**.

3.17.2 Opérations

Un rapport au sujet des opérations peut inclure n'importe quel ensemble de widgets du tableau de bord (p. 42) **Opérations**. Par défaut, tous les widgets présentent un résumé concernant le locataire 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. Tous les widgets présentent les paramètres 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.



Les rapports par défaut sont répertoriés ci-dessous :

Nom du rapport	Description	Disponible dans l'édition service
Alertes	Affiche les alertes survenues pendant une période donnée.	Cyber Backup, Cyber Protect
Détails de l'analyse de la sauvegarde	Affiche des informations détaillées au sujet des menaces détectées dans les sauvegardes.	Cyber Protect
Score CyberFit par périphérique	Affiche le Score CyberFit ainsi qu'une combinaison de ses indicateurs pour chaque périphérique.	Cyber Protect
Activités quotidiennes	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.	Cyber Backup, Cyber Protect
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.	Cyber Protect
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.	Cyber Backup, Cyber Protect
Machines découvertes	Affiche toutes les machines trouvées dans le réseau de l'organisation.	Cyber Backup, Cyber Protect

Prévision de l'intégrité du disque dur	Affiche des prévisions concernant le moment où votre disque dur/SSD tombera en panne, ainsi que l'état actuel des disques.	Cyber Protect
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.	Cyber Backup, Cyber Protect
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	Cyber Protect
Résumé	Affiche des informations résumées au sujet des périphériques protégés pendant une période donnée.	Cyber Backup, Cyber Protect
Activités hebdomadaires	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.	Cyber Backup, Cyber Protect

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

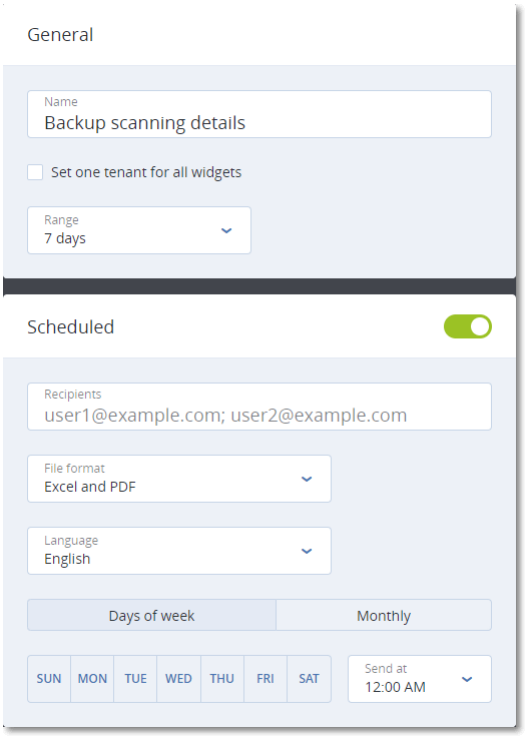
1. Cliquez sur **Ajouter un rapport**.
2. Effectuez l'une des actions suivantes :
   - Pour ajouter un rapport prédéfini, cliquez sur son nom.
   - Pour ajouter un rapport personnalisé, cliquez sur **Personnalisé**, cliquez sur le nom du rapport (les noms attribués par défaut sont similaires à **Personnalisé(1)**),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

Modification d'un 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
- 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 .xlsx



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, .xlsx 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**.

Vidage mémoire des données du rapport

Vous pouvez envoyer un vidage mémoire des données du rapport dans un fichier .csv par courrier électronique. 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 elliptique verticale dans le coin 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**.

3.17.3 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.

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 > 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 > Notifications du statut de cyberprotection	▪ Ce rapport est envoyé lorsqu'une activité est terminée. ***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.

3.18 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
- 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 votre centre de données Axproo, et leur disponibilité ne peut pas être affectée par des problèmes survenant sur les machines 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, **Locataire créé**, **Locataire supprimé**, **Utilisateur créé**, **Utilisateur supprimé**, **Quota atteint**.
- **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, **Locataire créé**, **Utilisateur créé**, **Utilisateur mis à jour**.

- **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 une 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 description, gravité ou date. Vous pouvez également rechercher les événements par objet, unité, initiateur et unité d'initiateur.

4 Scénarios avancés

4.1 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.

Restrictions

- Un locataire partenaire/dossier peut être déplacé uniquement vers un locataire partenaire/dossier.
- Un locataire client peut être déplacé uniquement vers un locataire partenaire/dossier.
- Un locataire unité ne peut pas être déplacé.

- Un locataire peut être déplacé uniquement si le locataire parent de destination possède le même ensemble de services et éléments, ou un plus grand, que le locataire parent d'origine.
- Les locataires ne peuvent être déplacés qu'au sein d'une seule hiérarchie de compte partenaire. Le déplacement de clients entre hiérarchies de compte partenaire n'est pas pris en charge.
- 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.

Comment déplacer un locataire

1. Connectez-vous au portail de gestion.
2. Dans l'onglet **Clients**, sélectionnez le locataire de destination vers lequel vous souhaitez déplacer un locataire.
3. Dans le volet Propriétés du locataire, cliquez sur l'icône en forme de points de suspension verticaux, puis sur **Afficher l'identifiant**.
4. Copiez la chaîne de texte affichée dans le champ **Identifiant interne**, puis cliquez sur **Annuler**.
5. Dans l'onglet **Clients**, sélectionnez le locataire que vous souhaitez déplacer.
6. Dans le volet Propriétés du locataire, cliquez sur l'icône elliptique verticale, puis sur **Déplacer**.
7. Coller l'identificateur interne du locataire de destination, puis cliquez sur **Déplacer**.

4.2 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 (p. 42) 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.

4.3 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 (p. 19) 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**.

4.4 Limitez l'accès à votre locataire

Les administrateurs de niveau client ou supérieur peuvent limiter l'accès des administrateurs de niveau supérieur à leurs locataires.

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. Cliquez sur **Paramètres** > **Sécurité**.
3. Désactivez le commutateur **Accès à l'assistance**.

4.5 Intégration à des systèmes tiers

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

- En définissant une extension de plate-forme dans ce système (p. 64).

  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 (p. 64) 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.

4.5.1 Configuration d'une extension Axproo Cyber Cloud

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres** > **Intégration**.
3. Cliquez sur le nom du système tiers avec lequel vous souhaitez activer l'intégration.
4. Suivez les instructions affichées à l'écran.

Vous trouverez davantage d'informations sur l'intégration avec des systèmes tiers dans la section « Références relatives à l'intégration » sur le site Web de Axproo.

4.5.2 Gestion des clients d'API

Des systèmes tiers peuvent être intégrés à Axproo Cyber Cloud 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.Axproo.com/doc/platform/management/v2.

4.5.2.1 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**.

4.5.2.2 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**.

4.5.2.3 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.

4.5.2.4 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.

4.5.2.5 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.*