

Portail de gestion

25.05

Table des matières

À propos de ce document	6
À propos du portail de gestion	7
Navigateurs Web pris en charge	7
Ma boîte de réception	7
Vue d'ensemble	7
Vérification de vos notifications	8
Recherche dans Ma boîte de réception	8
Comptes et unités	8
Gestion des quotas	9
Afficher les quotas pour votre organisation	10
Quotas principaux pour vos utilisateurs	17
Instructions pas-à-pas	20
Activation d'un compte administrateur	20
Exigences relatives au mot de passe	20
Accès au portail de gestion et aux services	21
Passer du portail de gestion aux consoles de service, et vice-versa	21
Navigation dans le portail de gestion	21
Création d'une unité	22
Création d'un compte utilisateur	22
Rôles utilisateur disponibles pour chaque service	25
Rôle d'administrateur en lecture seule	27
Rôle d'opérateur de restauration	28
La modification des paramètres de notification pour un utilisateur	29
Paramètres de notification par défaut activés par type de notification et rôle de l'utilisateur	31
Notifications activées par défaut par type de terminal et rôle d'utilisateur	32
Désactivation et activation d'un compte utilisateur	33
Suppression d'un compte utilisateur	33
Transférer la propriété d'un compte utilisateur	34
Configurer l'authentification à deux facteurs	35
Fonctionnement	35
Propagation de la configuration de l'authentification à deux facteurs à tous les niveaux de tenants	37
Configuration de l'authentification à deux facteurs pour vos tenants	38
Gestion de l'authentification à 2 facteurs pour les utilisateurs	39
Réinitialisation de l'authentification à deux facteurs en cas de perte du terminal qui applique	41

le second facteur	
Protection contre les attaques en force brute	41
Configuration des mises à jour de l'agent Cyber Protection	42
Stockage immuable	46
Modes de stockage immuable	47
Stockages et agents pris en charge	47
Configuration d'un stockage immuable	47
Affichage de l'utilisation du stockage immuable	49
Exemple de facturation pour le stockage immuable	50
Activation de la formation avancée de sensibilisation à la sécurité pour les utilisateurs de votre organisation	50
Limitation de l'accès à l'interface Web	51
Limitez l'accès à votre société	52
Gestion des tâches	53
Affichage des tickets auprès du service d'assistance	53
Création d'un ticket auprès du service d'assistance	53
Mise à jour des tickets auprès du service d'assistance	55
Soumission de tickets de service d'assistance via le portail de tickets	56
Surveillance	58
Utilisation	58
Tableau de bord des opérations	59
État de protection	60
Score #CyberFit par machine	61
Widgets de Endpoint Detection and Response (EDR)	61
Surveillance de l'intégrité du disque	64
Carte de la protection des données	68
Widgets d'évaluation des vulnérabilités	69
Widgets d'installation des correctifs	71
Détails de l'analyse de la sauvegarde	72
Affectés récemment	73
URL bloquées	74
Widget d'inventaire du logiciel	74
Widgets d'inventaire du matériel	75
Historique des sessions	76
Widget de suivi de la géolocalisation	76
Widget de sessions de chat	76
Widget de performance du technicien	77

Journal d'audit	77
Champs de journal d'audit	77
Filtrer et rechercher	79
Collecte de données de performances pour les agents Cyber Protection	79
Configuration des seuils de performances pour la collecte de données ETL	81
Rapports	83
Rapports d'utilisation	83
Type de rapport	83
Champ d'application du rapport	83
Indicateurs avec zéro utilisation	84
Configuration de rapports d'utilisation planifiés	84
Configuration de rapports d'utilisation personnalisés	84
Données des rapports d'utilisation	85
Rapports d'opération	85
Actions relatives aux rapports	87
Synthèse	89
Widgets de synthèse	90
Configuration des paramètres du rapport de synthèse	99
Création d'un rapport de synthèse	100
Personnalisation du rapport de synthèse	101
Envoi des rapports de synthèse	102
Fuseaux horaires dans les rapports	102
Données rapportées en fonction du type de widget	103
Intégrations	107
Catalogues des intégrations	107
Entrées du catalogue	108
Ouverture de votre catalogue des intégrations du centre de données	108
Ouverture du catalogue d'applications	109
Activation d'une intégration	113
Configuration d'une intégration active	113
Désactivation d'une intégration active	113
Clients de l'API	114
Identifiants du client d'API	114
Flux du client d'API	114
Création d'un client d'API	115
Réinitialisation de la valeur secrète d'un client d'API	115
Désactiver un client d'API	116

Activation d'un client d'API désactivé	116
Suppression d'un client d'API	116
Création d'une intégration	117
Index	118

À propos de ce document

Ce document est conçu pour les administrateurs client qui souhaitent se servir du portail de gestion Cloud pour créer et gérer les comptes, les unités et les quotas des utilisateurs, configurer et contrôler les accès, et surveiller l'utilisation et les opérations dans leur organisation Cloud.

À propos du portail de gestion

Le portail de gestion est une interface Web de la plate-forme Cloud qui fournit des services de protection de données.

Alors que chaque service possède sa propre interface Web, appelée Console de service, le portail de gestion permet aux administrateurs de contrôler l'utilisation des services, de créer des comptes utilisateur et des unités, de générer des rapports, et bien plus.

Navigateurs Web pris en charge

L'interface Web prend en charge les navigateurs suivants :

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

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

Ma boîte de réception

La page Ma boîte de réception est conçue pour rationaliser votre communication au sein de l'application. En suivant ce guide, vous pouvez gérer efficacement vos messages, rester organisé et améliorer votre productivité. La boîte de réception de la solution est le centre névralgique dans lequel vous recevez et gérez les communications au sein de l'application. Elle vous permet de rester informé des mises à jour, des messages et des alertes importants dans votre workflow.

Vue d'ensemble

L'onglet **Ma boîte de réception** comporte un compteur de notifications qui affiche le nombre de notifications non lues. En cliquant sur ce compteur, vous pouvez afficher les notifications non lues et suivre facilement les éléments en attente. En outre, les compteurs situés à côté de chacun des filtres (catégorie, importance, action) permettent de connaître la répartition des notifications dans les différentes catégories.

Vous recevrez dans votre boîte de réception des notifications de différents types correspondant au contexte et aux objectifs spécifiques définis dans les paramètres de compte : annonces de fonctionnalités, nouveaux programmes de formation disponibles, invitations à des événements et des webinaires, rappels d'expiration de certificat, promotions, avis de maintenance, enquêtes, etc.

Vérification de vos notifications

Vérification de votre section de notification

1. Connectez-vous à la console Cyber Protect Cloud.
2. Dans le volet de navigation, sélectionnez l'option de menu **Ma boîte de réception**.

Recherche dans Ma boîte de réception

Pour rechercher des messages non lus

1. Cliquez sur l'option de menu **Ma boîte de réception**.
2. Dans l'angle supérieur droit, activez le bouton **Afficher uniquement les éléments non lus**.

Pour rechercher des informations importantes dans votre boîte de réception

1. Accédez à **Ma boîte de réception** depuis le tableau de bord Cyber Protect Cloud.
2. Dans la vue de la boîte de réception, localisez la **barre de recherche**, en haut.
3. Saisissez les mots-clés ou les noms d'expéditeur pertinents pour filtrer les messages.
4. Appuyez sur la touche **Entrée** pour afficher les résultats de la recherche.

Les résultats affichent toutes les notifications correspondant à vos critères de recherche.

Comptes et unités

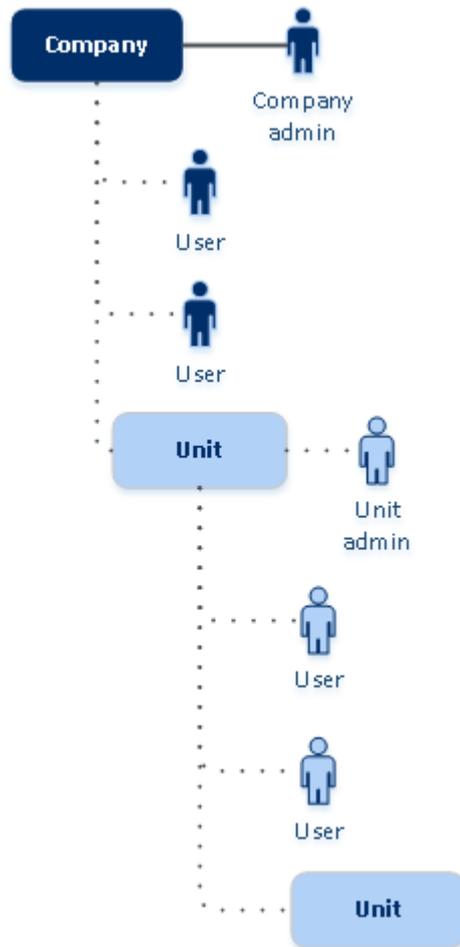
Il existe deux types de comptes utilisateur : les comptes administrateur et les comptes utilisateur.

- 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.

Les administrateurs peuvent créer des unités, qui correspondent généralement à des unités ou des départements de l'organisation. Chaque compte existe soit au niveau de la société, soit dans une unité.

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

Le diagramme ci-dessous présente trois niveaux de hiérarchie : la société et deux unités. Les unités et les comptes facultatifs sont signalés par une ligne en pointillés.



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

Opération	Utilisateurs	Administrateurs
Créer des unités	Non	Oui
Créer des comptes	Non	Oui
Téléchargez et installez le logiciel	Oui	Oui
Utilisez les services	Oui	Oui
Créer des rapports concernant l'utilisation du service	Non	Oui

Gestion des quotas

Les quotas limitent les possibilités d'utilisation du service par le tenant.

Dans votre portail de gestion, vous pouvez afficher les quotas de service que votre fournisseur de service a alloués à votre organisation, mais vous ne pouvez pas les gérer.

Vous pouvez gérer les quotas de service pour vos utilisateurs.

Important

Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

Afficher les quotas pour votre organisation

Dans le portail de gestion, accédez à **Vue d'ensemble > Utilisation**. Vous verrez un tableau de bord affichant les quotas alloués à votre organisation. Les quotas pour chaque service s'affichent dans un onglet différent.

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 terminaux

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

Une machine, un terminal 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 terminaux est atteint, l'utilisateur ne peut plus activer de plans de protection sur d'autres terminaux.

Quotas pour les sources de données Cloud

- **Postes Microsoft 365**
Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Les administrateurs d'entreprise peuvent afficher le quota et son utilisation dans le portail de gestion. Lorsque le quota inconditionnel est dépassé, les plans de sauvegarde ne peuvent pas être appliqués à de nouveaux postes.

La facturation de ce quota dépend du mode de facturation sélectionné pour Cyber Protection.

- En mode de facturation **Par gigaoctet**, la facturation est basée uniquement sur l'utilisation du stockage et les postes ne sont pas comptés.
- En mode de facturation **Par ressource**, la facturation est basée sur le nombre de postes Microsoft 365 protégés. L'utilisation du stockage est facturée uniquement pour les postes non protégés.

Le tableau suivant récapitule le mode de facturation **Par ressource**.

	Emplacement de sauvegarde	
	Stockage hébergé Acronis* Stockage hébergé par un partenaire	Stockage Microsoft Azure Stockage Google
Poste protégé	La facturation est établie en fonction du nombre de postes protégés. L'espace de stockage utilisé par les sauvegardes des postes protégés n'est pas facturé.	Les postes protégés et le stockage utilisé sont facturés.
Poste non protégé	Les postes non protégés ne sont pas facturés. L'espace de stockage utilisé par les sauvegardes des postes non protégés est facturé.	Les postes non protégés ne sont pas facturés. L'espace de stockage utilisé par les sauvegardes des postes non protégés est facturé.

* La politique d'utilisation équitable d'Acronis Storage s'applique. Les conditions générales sont disponibles sur <https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage>.

Un poste est considéré comme étant protégé lorsqu'un utilisateur Microsoft 365 dispose de l'un des éléments suivants :

- Boîte aux lettres à laquelle un plan de sauvegarde est appliqué
- Compte OneDrive auquel un plan de sauvegarde est appliqué
- Accès à une ressource protégée de l'entreprise : site Microsoft 365 SharePoint Online ou Microsoft 365 Teams.

Pour savoir comment contrôler le nombre de membres d'un site Microsoft 365 SharePoint ou Teams, reportez-vous à [cet article de la base de connaissances](#).

Un poste peut devenir non protégé dans les cas suivants :

- L'accès à une ressource protégée au niveau de l'entreprise, telle que Microsoft 365 SharePoint Online ou Microsoft 365 Teams, est révoqué pour un utilisateur.
- Tous les plans de sauvegarde sont révoqués de la boîte aux lettres ou du compte OneDrive d'un utilisateur.
- Un utilisateur est supprimé de l'organisation Microsoft 365.

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

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

Remarque

Les utilisateurs Microsoft 365 bloqués qui n'ont pas de boîte aux lettres personnelle ou de compte OneDrive protégé, et n'ont accès qu'aux ressources partagées (boîtes aux lettres partagées, sites SharePoint et Microsoft Teams), ne sont pas facturés. Les utilisateurs bloqués sont ceux qui n'ont pas de connexion valide et ne peuvent pas accéder aux services Microsoft 365. Pour savoir comment bloquer tous les utilisateurs non autorisés d'une organisation Microsoft 365, voir "Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter" (p. 15).

Important

L'agent local et l'agent dans le cloud consomment des quotas distincts. Si vous sauvegardez les mêmes ressources à l'aide des deux agents, vous êtes facturé deux fois. Par exemple :

- Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et les fichiers OneDrive de ces mêmes utilisateurs à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.
 - Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et également à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.
-

Pour consulter les questions fréquentes sur l'attribution de licences Microsoft 365, voir [Cyber Protect Cloud : licence Microsoft 365 par Go](#) et [Cyber Protect Cloud : modifications des licences et des tarifs Microsoft 365](#).

- **Microsoft 365 SharePoint Online**

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

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

- **Microsoft 365 Teams**

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

- **Postes d'archivage d'e-mails Microsoft 365**

Le quota **Postes d'archivage des e-mails Microsoft 365** active ou désactive la possibilité de créer une archive d'e-mails pour les serveurs de messagerie Microsoft 365 et définit le nombre maximal de boîtes aux lettres pouvant être ajoutées à l'archive.

- **Postes d'archivage des e-mails (obsolète)**

Ce quota est obsolète et vous ne pouvez pas l'activer lors de la création de nouveaux tenants dans le portail de gestion.

Pour les tenants existants, vous pouvez uniquement désactiver le quota s'il était déjà activé, mais vous ne pouvez plus l'activer.

Important

Lors de la création de nouveaux tenants clients, utilisez le quota de **Postes d'archivage Microsoft 365**.

Pour les clients existants, le quota de **Postes d'archivage des e-mails (obsolète)** sera automatiquement remplacé par le quota de **Postes d'archivage Microsoft 365**. Toute utilisation existante sous **Postes d'archivage des e-mails (obsolète)** sera transférée vers **Postes d'archivage Microsoft 365**.

Postes Google Workspace

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

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

Lorsque le quota inconditionnel est dépassé, un administrateur d'entreprise ne peut pas appliquer un plan de sauvegarde à de nouveaux postes.

- **Drive partagé Google Workspace**

Ce quota est appliqué par le fournisseur de services à l'ensemble de l'entreprise. Ce quota active ou désactive la capacité à protéger des Drive partagés Google Workspace. Si le quota est activé, un nombre illimité de Drive partagés peut être protégé. Les administrateurs de l'entreprise ne peuvent pas consulter le quota dans le portail de gestion, mais peuvent consulter la quantité de stockage occupée par les sauvegardes de Drive partagé dans les rapports d'utilisation.

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

Quotas pour le stockage

Important

Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

• Ressources Cloud

◦ Stock. de sauvegarde

▪ Stock. de sauvegarde

Ce quota limite la taille totale des sauvegardes stockées dans le cloud. Lorsque le quota inconditionnel de stockage de sauvegarde est dépassé, l'opération de sauvegarde ne démarre pas.

Dans le mode de facturation **Par ressource**, ce quota s'applique uniquement aux sauvegardes de ressources différentes de Microsoft 365 et Google Workspace.

Le stockage de sauvegarde pour les ressources Microsoft 365 et Google Workspace est illimité*. Si un quota de poste, tel que les **Postes Microsoft 365** ou les **Postes Google Workspace**, est supprimé d'une ressource, le stockage de sauvegarde reste illimité, mais son utilisation sera facturée.

En mode de facturation **Par gigaoctet**, ce quota s'applique à toutes les sauvegardes, y compris celles des ressources Microsoft 365 et Google Workspace.

* La politique d'utilisation équitable d'Acronis Storage s'applique. Les conditions générales sont disponibles sur <https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage>.

▪ Stockage d'archives

Ce quota limite la taille totale de l'archive d'e-mails dans l'infrastructure cloud.

◦ Advanced Disaster Recovery

Cette section contient les quotas liés à la reprise d'activité après sinistre.

• Ressources locales

◦ Sauvegarde locale

La **Sauvegarde locale** est soumise à un quota qui limite la taille totale des sauvegardes vers des disques locaux, des partages réseau et des clouds publics tels que les services compatibles S3, Azure, AWS, Wasabi et Impossible Cloud.

- Aucun dépassement ne peut être défini pour ce quota.

- Le quota inconditionnel ne peut pas être appliqué aux sauvegardes locales.

Remarque

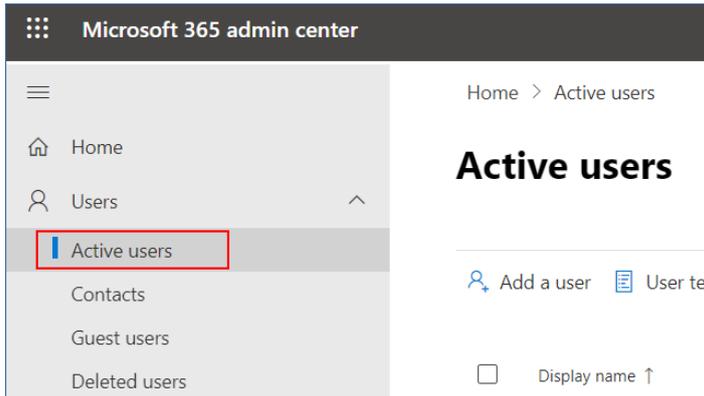
Désactiver le quota de **Sauvegarde locale** désactivera les sauvegardes locales, les sauvegardes vers des partages réseau et vers les clouds publics.

Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter

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

Pour empêcher les utilisateurs sans licence de se connecter

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



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



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



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

Quotas de Disaster Recovery

Remarque

Les éléments de Disaster Recovery ne sont disponibles qu'avec le module complémentaire de 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**

Le stockage de reprise d'activité après sinistre affiche la taille du stockage des sauvegardes des serveurs protégés avec la reprise d'activité après sinistre. L'utilisation du stockage de reprise d'activité après sinistre correspond à l'utilisation du stockage des sauvegardes des ressources

protégées avec des serveurs de reprise d'activité après sinistre. Ce stockage est calculé à partir du moment où un serveur de restauration est créé, qu'il soit en cours d'exécution ou non. Si le quota est dépassé, il ne sera pas possible de créer des serveurs primaires et de restauration, ni d'ajouter/étendre des disques des serveurs primaires existants. Si la surconsommation de ce quota est dépassée, il ne sera pas possible d'initier un basculement ni de 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 Cyber Protect, mais seule l'option **Supprimer** est disponible.

- **Accès Internet**

Ce quota active ou désactive l'accès à Internet à partir de serveurs primaires ou de restauration.

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

Quotas pour la File Sync & Share

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.

- **Utilisateurs**

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

Les comptes administrateur ne sont pas comptabilisés dans ce quota.

- **Stockage dans le Cloud**

Il s'agit d'un stockage dans le Cloud, destiné à stocker les fichiers des utilisateurs. Le quota définit l'espace alloué à un tenant dans le stockage dans le Cloud.

Quotas d'envoi de données physiques

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

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.

- **Vers le Cloud**

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

Quotas pour Notary

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.

- **Stockage Notary**

Définit l'espace maximal de stockage dans le cloud des fichiers notariés, des fichiers signés et de ceux dont la notarisation ou la signature est en cours.

Pour réduire l'utilisation de ce quota, vous pouvez supprimer les fichiers déjà notariés ou signés du stockage de notarisation.

- **Notarisations**

Définit le nombre maximal de fichiers pouvant être notariés à l'aide du service de notarisation.

Un fichier est considéré comme étant 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**

Définit le nombre maximal de signatures électroniques numériques.

Quotas principaux pour vos utilisateurs

Les **quotas** vous permettent de limiter la capacité d'un utilisateur à utiliser le service. Pour définir les quotas d'un utilisateur, sélectionnez ce dernier dans l'onglet **Utilisateurs**, sous **Mon entreprise**, puis cliquez sur l'icône représentant un crayon dans la section **Quotas**.

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 conditionnel : Vous avez défini le quota des postes de travail sur 20. Lorsque le nombre de postes de travail protégés de l'utilisateur atteint 20, il reçoit une notification par e-mail, mais le service Cyber Protection reste disponible.

Quota inconditionnel : Si vous avez défini le quota de postes de travail sur 20 et que le dépassement est de 5, l'utilisateur 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.

Quotas de sauvegarde

Vous pouvez indiquer le quota de stockage de sauvegarde et le nombre maximum de machines/terminaux/sites Web qu'un utilisateur est autorisé à protéger. Les quotas suivants sont disponibles.

Quotas pour les terminaux

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

Une machine, un terminal 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 terminaux est atteint, l'utilisateur ne peut plus activer de plans de protection sur d'autres terminaux.

Quota pour le stockage

Important

Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

- **Stockage de sauvegarde**

Le quota de stockage des sauvegardes limite la taille totale des sauvegardes situées dans le stockage dans le Cloud. Lorsque le quota de stockage des sauvegardes est dépassé, les sauvegardes échouent.

Important

L'agent local et l'agent dans le cloud consomment des quotas distincts. Si vous sauvegardez les mêmes ressources à l'aide des deux agents, vous êtes facturé deux fois. Par exemple :

- Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et les fichiers OneDrive de ces mêmes utilisateurs à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.
 - Si vous sauvegardez les boîtes aux lettres de 120 utilisateurs à l'aide de l'agent local et également à l'aide de l'agent dans le cloud, vous êtes facturé pour 240 postes Microsoft 365.
-

Quotas pour la File Sync & Share

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

- **Espace de stockage personnel**

Définit l'espace de stockage dans le cloud alloué aux fichiers d'un utilisateur.

Quotas pour Notary

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

- **Stockage Notary**

Définit l'espace maximal de stockage dans le cloud des fichiers notariés, des fichiers signés et de ceux dont la notarisation ou la signature est en cours.

Pour réduire l'utilisation de ce quota, vous pouvez supprimer les fichiers déjà notariés ou signés du stockage de notarisation.

- **Notarisations**

Définit le nombre maximal de fichiers pouvant être notariés à l'aide du service de notarisation.

Un fichier est considéré comme étant 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**

Définit le nombre maximal de signatures électroniques numériques.

Instructions pas-à-pas

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

- Activer votre compte administrateur
- Accédez au portail de gestion et aux services
- Créez une unité
- Créez un compte utilisateur

Activation d'un compte administrateur

Après avoir contracté un service, vous recevrez un e-mail contenant les informations suivantes :

- **Votre identifiant.** Nom d'utilisateur que vous utilisez pour vous connecter. Votre identifiant figure également sur la page d'activation du compte.
- Bouton **Activer le compte.** Cliquez sur le bouton et définissez le mot de passe de votre compte. Assurez-vous que votre mot de passe comporte au moins neuf caractères. Pour en savoir plus sur le mot de passe, consultez "Exigences relatives au mot de passe" (p. 20).

Exigences relatives au mot de passe

La complexité des mots de passe est vérifiée lors de l'inscription de l'utilisateur et les mots de passe sont classés dans l'une des catégories suivantes :

- Faible
- Moyenne
- Fort

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

Remarque

Les exigences en matière de mot de passe sont susceptibles de changer.

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

Accès au portail de gestion et aux services

1. Accédez à la page de connexion de la console de service.
2. Saisissez l'identifiant, puis cliquez sur **Suivant**.
3. Saisissez le mot de passe, puis cliquez sur **Suivant**.
4. Effectuez l'une des actions suivantes :
 - Pour vous connecter au service de sauvegarde, cliquez sur **Portail de gestion**.
 - Pour vous connecter à un service, cliquez sur le nom du service.

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

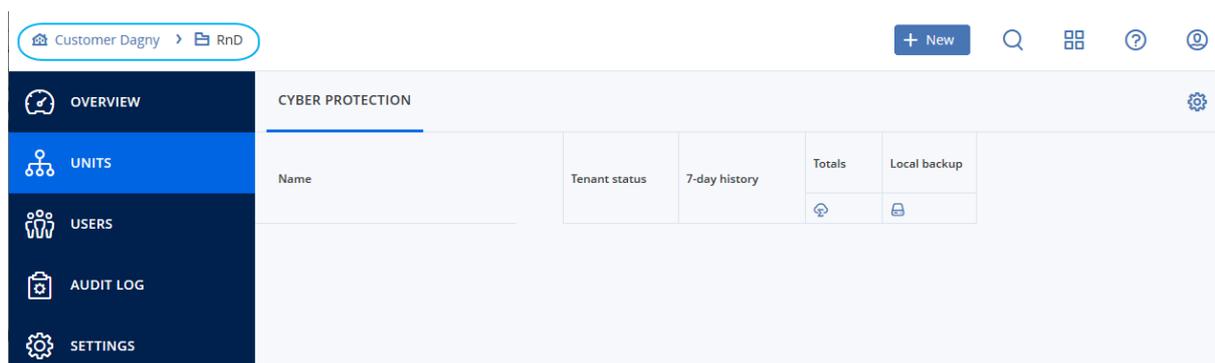
Passer du portail de gestion aux consoles de service, et vice-versa

Pour passer du portail de gestion aux consoles de service, et vice-versa, cliquez sur l'icône  dans l'angle supérieur droit, puis sélectionnez **Portail de gestion** ou le service auquel vous souhaitez accéder.

Navigation dans le portail de gestion

Lorsque vous utilisez le portail de gestion, vous travaillez au sein de la société ou d'une unité 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 de l'unité 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 la société ou l'unité dans laquelle vous travaillez actuellement. Par exemple :

- En utilisant le bouton **Nouveau**, vous pouvez créer une unité ou un compte utilisateur uniquement dans cette société ou unité.

- L'onglet **Unités** affiche uniquement les unités qui sont des enfants directs de cette société ou unité.
- L'onglet **Utilisateurs** affiche uniquement les comptes client existant dans cette société ou unité.

Création d'une unité

Ignorez cette étape si vous ne souhaitez pas organiser de comptes en unités.

Si vous prévoyez de créer des unités ultérieurement, veuillez noter que les comptes existants ne peuvent pas être déplacés entre les unités ou entre la société et les unités. Vous devez d'abord créer une unité, puis la remplir de comptes.

Pour créer une unité

1. Connectez-vous au portail de gestion.
2. Naviguez vers l'unité dans laquelle vous souhaitez créer une unité.
3. Dans l'angle supérieur droit, cliquez sur **Nouveau > Unité**.
4. Dans la section **Nom**, indiquez le nom de la nouvelle unité.
5. [Facultatif] Dans **Langue**, changez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée au sein de cette unité.
6. Effectuez l'une des actions suivantes :
 - Pour créer un administrateur d'unité, cliquez sur **Suivant**, puis suivez les étapes décrites dans [« Création d'un compte utilisateur »](#) à partir de l'étape 4.
 - Pour créer une unité sans administrateur, cliquez sur **Enregistrer et fermer**. Vous pourrez ajouter des administrateurs et des utilisateurs à l'unité ultérieurement.

L'unité nouvellement créée s'affiche dans l'onglet **Unités**.

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

Création d'un compte utilisateur

Vous pouvez créer des comptes supplémentaires dans les cas suivants :

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

Pour créer un compte utilisateur

1. Connectez-vous au portail de gestion.
2. Naviguez vers l'unité dans laquelle vous souhaitez créer un compte utilisateur.
3. Dans l'angle supérieur droit, cliquez sur **Nouveau > Utilisateur**.
Vous pouvez également accéder à **Mon entreprise > Utilisateurs** et cliquer sur **+ Nouveau**.
4. Indiquez les informations de contact suivantes relatives au compte :
 - . Si vous préférez utiliser un identifiant de connexion différent de l'adresse e-mail, cochez la case **Utilisez un identifiant différent de votre adresse e-mail**, puis entrez l'**identifiant** et l'**adresse e-mail**.

Important

Si l'utilisateur est enregistré dans le service File Sync & Share, indiquez l'adresse e-mail qui a été utilisée pour l'inscription File Sync & Share.

Veillez noter que chaque compte utilisateur du client doit disposer d'une adresse e-mail unique.

Important

Chaque compte doit disposer d'un identifiant unique.

- [Facultatif] **Prénom**
 - [Facultatif] **Nom**
 -
 - Dans le champ **Langue**, changez la langue par défaut des notifications, des rapports et du logiciel qui sera utilisée pour ce compte.
5. [Facultatif] Indiquez les contacts d'entreprise.
 - **Facturation** : contact qui recevra les mises à jour concernant les modifications importantes relatives aux rapports d'utilisation dans la plate-forme.
 - **Technique** : contact qui recevra les mises à jour concernant les modifications techniques importantes dans la plate-forme.
 - **Professionnel** : contact qui recevra les mises à jour concernant les modifications importantes relatives à l'activité dans la plate-forme.

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

Vous pouvez afficher les contacts d'entreprise affectés pour un utilisateur de la liste **Utilisateurs**, dans la colonne **Contacts de l'entreprise**, puis modifiez le compte utilisateur afin de changer les contacts d'entreprise si nécessaire.
 6. [Non disponible lors de la création d'un compte dans un partenaire / dossier tenant]
Sélectionnez les services auxquels l'utilisateur aura accès et les rôles dans chaque service.
Les services disponibles dépendent des services activés pour le tenant 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 tenant. L'utilisateur aura le rôle d'administrateur dans tous les services qui seront activés

pour le tenant 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.
- Sinon, l'utilisateur recevra les rôles que vous choisirez dans les services que vous activerez pour cet utilisateur.

7. Cliquez sur **Créer**.

Le compte utilisateur qui vient d'être créé s'affiche dans l'onglet **Utilisateurs**, sous **Mon entreprise**.

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

Réinitialiser le mot de passe d'un utilisateur

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

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

Le compte peut désormais être utilisé pour les services qui ne prennent pas en charge l'authentification à deux facteurs (par exemple, l'inscription dans Cyber Infrastructure) ; vous devrez peut-être convertir un compte utilisateur en *compte de service* — un compte qui ne nécessite pas d'authentification à deux facteurs.

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

Pour convertir un compte utilisateur en un compte de service

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

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

Rôles utilisateur disponibles pour chaque service

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

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

Remarque

Les services disponibles sont configurés par votre fournisseur de services.

Service	Rôle	Description
N/D	Administrateur d'entreprise	Ce rôle accorde des droits d'administrateur complets pour tous les services. Ce rôle donne accès à la liste d'autorisation de l'entreprise. Si le module complémentaire de Disaster Recovery du service de protection est activé pour l'entreprise, ce rôle donne également accès à la fonctionnalité de reprise d'activité après sinistre.
	Administrateur de l'unité Niveau unité	Ce rôle accorde les autorisations les plus élevées possibles à tous les services applicables dans l'unité. Le rôle ne permet cependant pas l'accès aux fonctionnalités de reprise d'activité après sinistre.
Portail de gestion	Administrateur	Ce rôle donne accès au portail de gestion, où l'administrateur peut gérer les utilisateurs dans l'ensemble de l'organisation.
	Administrateur en lecture seule	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion de toute l'entreprise. Voir "Rôle d'administrateur en lecture seule" (p. 27).
	Administrateur en lecture seule Niveau unité	Ce rôle fournit un accès en lecture seule à tous les objets du portail de gestion de l'unité et des sous-unités de l'entreprise. Voir "Rôle d'administrateur en lecture seule" (p. 27).
Portail dédié aux fournisseurs	Développeur	Ce rôle fournit un accès complet au portail dédié aux fournisseurs. Les développeurs peuvent créer et gérer des applications CyberApp, CyberApp Descriptions et CyberApp Versions. Ils peuvent également soumettre des demandes de déploiement et surveiller les indicateurs CyberApp.
	Utilisateur	Ce rôle permet à l'utilisateur de créer, de gérer et de demander des approbations de CyberApp Descriptions.
	Utilisateur en lecture seule	Ce rôle fournit un accès en lecture seule au portail dédié aux fournisseurs.

Protection	Administrateur	<p>Ce rôle active la configuration et la gestion du service de protection pour vos clients.</p> <p>Ce rôle est requis pour :</p> <ul style="list-style-type: none"> • la configuration et la gestion de la fonctionnalité Disaster Recovery. • la configuration et la gestion de la liste d'autorisation de l'entreprise. • l'exécution de la découverte automatique des terminaux. • toutes les actions liées au déploiement de logiciels à l'aide de DeployPilot (utilisation des plans de déploiement, des référentiels et des packages de logiciels, et réalisation d'actions de déploiement rapide).
	Cyberadministrateur	<p>Outre l'attribution de droits d'administrateur, ce rôle permet de configurer et de gérer le service de protection, et d'approuver des actions dans la création de cyberscripts.</p> <p>Le rôle Cyberadministrateur n'est disponible que pour les tenants pour lesquels le pack Advanced Management (RMM) est activé.</p>
	Administrateur en lecture seule	<p>Ce rôle fournit un accès en lecture seule à tous les objets du service de protection. Voir "Rôle d'administrateur en lecture seule" (p. 27).</p>
	Utilisateur	<p>Ce rôle permet d'utiliser le service de protection, mais sans privilèges d'administrateur, et d'accéder à des fonctionnalités telles qu'EDR (Endpoint Detection and Response). Toutefois, les utilisateurs bénéficiant de ce rôle ne peuvent pas accéder aux données des autres utilisateurs de l'organisation.</p>
	Opérateur de restauration	<p>Applicable aux organisations Microsoft 365 et Google Workspace, le rôle permet d'accéder aux sauvegardes et d'en autoriser la restauration, tout en restreignant l'accès au contenu sensible à l'intérieur des sauvegardes. Voir "Rôle d'opérateur de restauration" (p. 28).</p>
	Analyste de sécurité	<p>Le rôle peut être affecté uniquement dans les tenants de clients pour lesquels le pack Advanced Security + EDR ou Advanced Security + XDR est activé. Il fournit l'accès à la console de cyberprotection, et permet à l'utilisateur de gérer les incidents EDR et de prendre des mesures d'intervention.</p>
File Sync & Share	Administrateur	<p>Ce rôle permet de configurer et de gérer le service File Sync & Share pour vos utilisateurs.</p>
Cyber Infrastructure	Administrateur	<p>Ce rôle permet de configurer et de gérer Cyber Infrastructure pour vos utilisateurs.</p>

Notary	Administrateur	Ce rôle permet de configurer et de gérer Notary pour vos utilisateurs.
	Utilisateur	Ce rôle permet d'utiliser le service Notary, mais sans droits d'accès d'administrateur. Ces utilisateurs ne peuvent pas accéder aux données des autres utilisateurs de l'organisation.

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

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

Rôle d'administrateur en lecture seule

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

- Collecter des données de diagnostic, comme les rapports système.
- Voir les points de restauration d'une sauvegarde, mais pas explorer le contenu de la sauvegarde ni voir les fichiers, dossiers ou e-mails.
- Lorsque la fonctionnalité Advanced Security + XDR est activée, les administrateurs en lecture seule peuvent accéder à l'onglet Mesures d'intervention dans l'écran des incidents EDR, mais ils ne peuvent exécuter aucune action.
- L'accès aux données des autres utilisateurs de l'organisation est en mode lecture seule.

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

- Démarrer ou arrêter une tâche.
Par exemple, un administrateur en lecture seule ne peut pas démarrer une restauration ou arrêter une sauvegarde en cours d'exécution.
- Configurer et gérer la fonctionnalité Disaster Recovery ni la liste d'autorisation de l'entreprise, et dispose d'un accès en lecture seule aux plans de déploiement, aux référentiels et aux packages de logiciels.
- Accéder au système de fichiers sur les ordinateurs source ou cible.
Par exemple, un administrateur en lecture seule ne peut pas voir de fichiers, dossiers ou e-mails sur un ordinateur sauvegardé.
- Changer des paramètres.
Par exemple, un administrateur en lecture seule ne peut pas créer de plan de protection ni modifier l'un de ses paramètres.
- Créer, mettre à jour ni supprimer de données.
Par exemple, un administrateur en lecture seule ne peut pas supprimer de sauvegardes.

Remarque

Dans le portail de gestion, les administrateurs en lecture seule peuvent initier la création de nouveaux tenants enfants et configurer toutes leurs propriétés à des fins de démonstration, mais ils ne peuvent pas les enregistrer.

- Enregistrez toutes les modifications apportées aux plans de script, aux plans de surveillance ou aux plans d'agent.

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

Rôle d'opérateur de restauration

Remarque

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

Un opérateur de restauration peut effectuer les actions suivantes :

- Afficher les alertes et les activités
- Afficher et actualiser la liste des sauvegardes.
- Afficher la liste des points de restauration.
- Parcourir les sauvegardes sans accéder à leur contenu.

Remarque

Les opérateurs de restauration peuvent consulter les noms des fichiers sauvegardés ainsi que les objets et expéditeurs des e-mails sauvegardés.

- Rechercher des sauvegardes (recherche dans le texte intégral non prise en charge).
- Restaurer uniquement des sauvegardes cloud-à-cloud vers leur emplacement d'origine au sein de l'organisation Microsoft 365 ou Google Workspace d'origine.

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

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

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

La modification des paramètres de notification pour un utilisateur

Vous pouvez configurer les notifications qu'un utilisateur recevra par e-mail, si le service Cyber Protection est activé pour le tenant où l'utilisateur est créé.

Pour configurer les notifications pour un utilisateur

1. Accédez à **Mon entreprise > Utilisateurs**.
2. Cliquez sur l'utilisateur pour lequel vous souhaitez configurer les notifications, puis, dans l'onglet **Services**, dans la section **Notifications par e-mail**, cliquez sur l'icône de crayon.
3. Sélectionnez les cases à cocher des notifications par e-mail que vous souhaitez activer.

Notifications	Description
Notifications de maintenance	Notifications informant les utilisateurs partenaires, les tenants enfants (partenaires et clients) et les utilisateurs individuels des activités de maintenance à venir sur le centre de données Cyber Protect. Ces notifications peuvent être activées par les utilisateurs partenaires pour leurs tenants enfants, et par les utilisateurs partenaires ou les administrateurs de l'entreprise pour les utilisateurs individuels au sein de leur organisation.
Notifications relatives aux dépassements de quotas	Les notifications relatives aux dépassements de quotas.
Rapports d'utilisation planifiés	Rapports d'utilisation envoyés le premier jour de chaque mois.
Notifications de labellisation d'URL	Notifications concernant l'expiration prochaine du certificat utilisé pour l'URL personnalisée des services de Cyber Protect Cloud. Les notifications sont envoyées à tous les administrateurs du tenant sélectionné : 30 jours, 15 jours, 7 jours, 3 jours et 1 jour avant l'expiration du certificat.
Compte à rebours	Notifications concernant l'expiration de la version d'évaluation du

Notifications	Description
pour les notifications de bascule en production	clients qui seront envoyées 10 jours avant l'expiration de la version d'évaluation et 3 jours avant l'expiration de la version d'évaluation.
Notification d'activation du mode production	Notifications concernant l'activation du mode production.
Notifications d'échec	Les notifications relatives aux résultats d'exécution des plans de protection et aux résultats des opérations de reprise d'activité après sinistre pour chaque terminal.
Notifications d'avertissement	Les notifications relatives aux résultats d'exécution des plans de protection et aux résultats des opérations de reprise d'activité après sinistre pour chaque terminal.
Notifications de réussite	Les notifications relatives aux résultats d'exécution des plans de protection et aux résultats des opérations de reprise d'activité après sinistre pour chaque terminal.
Résumé quotidien des alertes actives	Le résumé quotidien est généré sur la base de la liste des alertes actives présentes dans la console Cyber Protect au moment de la génération du résumé. Le résumé est généré et envoyé une fois par jour entre 10:00 et 23:59 UTC. L'heure à laquelle le rapport est généré et envoyé dépend de la charge de travail du centre de données. S'il n'y a aucune alerte active, aucun résumé n'est envoyé. Le résumé n'inclut pas d'informations concernant les alertes passées qui ne sont plus actives. Par exemple, si un utilisateur trouve une sauvegarde échouée et supprime l'alerte, ou qu'il relance une sauvegarde et que celle-ci réussit avant que le résumé ne soit généré, l'alerte ne sera plus présente et le résumé ne l'affichera pas.
Notifications de contrôle des terminaux	Les notifications concernant les tentatives d'utilisation de périphériques et de ports restreints par des plans de protection avec le module de contrôle des terminaux activé.
Notifications concernant les nouveaux terminaux détectés	Notifications concernant les terminaux nouvellement détectés. Ces notifications sont envoyées tous les lundis et jeudis.
Notifications de restauration	Les notifications concernant les actions de restauration sur les ressources suivantes : messages e-mail et boîte aux lettres complètes d'utilisateurs, dossiers publics, OneDrive / GoogleDrive : OneDrive complet et fichiers ou dossiers, Fichiers SharePoint, Teams : canaux, équipes complètes, messages e-mail et sites d'équipe.

Notifications	Description
	Dans le cadre de ces notifications, les actions suivantes sont considérées comme des actions de restauration : envoi en tant qu'e-mail, téléchargement ou lancement d'une opération de restauration.
Notifications de prévention des pertes de données	Notifications concernant les alertes de prévention de la perte de données relatives à l'activité de cet utilisateur sur le réseau.
Notifications d'incident de sécurité	<p>Les notifications concernant la détection de malwares durant les analyses lors de l'accès, lors de l'exécution ou à la demande, et concernant les éléments détectés par le moteur de comportement et par le moteur de filtrage d'URL.</p> <p>Deux options sont disponibles : Atténuée et Non atténuée. Ces options s'appliquent aux alertes Endpoint Detection and Response (EDR) d'incident, aux alertes provenant de flux de menaces et à celles concernant les ressources sur lesquelles la fonctionnalité EDR n'est pas activée.</p> <p>Lors de la création d'une alerte EDR, un e-mail est envoyé à l'utilisateur pertinent. Si le statut de la menace identifiée dans l'incident change, un nouvel e-mail est envoyé. Les e-mails comportent des boutons d'action qui permettent à l'utilisateur de voir les détails de l'incident (s'il a été atténué), ou de mener une enquête et de traiter l'incident (s'il n'a pas été atténué).</p>
Notifications d'infrastructure	Notifications concernant des problèmes avec l'infrastructure de Disaster Recovery : lorsque l'infrastructure de Disaster Recovery ou les tunnels VPN ne sont pas disponibles.

Remarque

Les utilisateurs VMware Cloud Director peuvent recevoir les notifications suivantes : notifications relatives aux dépassements de quotas, rapports d'utilisation planifiés (si de tels rapports sont configurés pour l'organisation) et résumé quotidien des alertes actives.

Paramètres de notification par défaut activés par type de notification et rôle de l'utilisateur

Les notifications activées ou désactivées par défaut dépendent du type de notification et du rôle de l'utilisateur.

Types de notification\Rôle utilisateur	Client, administrateurs d'unité (libre-service)	Client, administrateurs d'unité (gérés par le fournisseur de services)
Notifications de	Non	Non

maintenance		
Notifications relatives aux dépassements de quotas	Oui	Non
Notifications de rapports d'utilisation planifiés	Oui	Non
Notifications de labellisation d'URL	Non	Non
Notifications d'échec	Non	Non
Notifications d'avertissement	Non	Non
Notifications de réussite	Non	Non
Résumé quotidien concernant les alertes actives	Oui	Non
Notifications de contrôle de terminal	Non	Non
Notifications de restauration	Non	Non
Notifications de prévention de perte de données	Non	Non
Notifications d'incidents de sécurité : Atténuées	Non	Non
Notifications d'incidents de sécurité : Non atténuées	Non	Non
Notifications d'infrastructure	Non	Non

Notifications activées par défaut par type de terminal et rôle d'utilisateur

Type de terminal\Rôle de l'utilisateur	Utilisateur	Administrateur client
Notifications pour tous les terminaux	Oui	Oui
Notifications pour tous les terminaux de votre organisation	N/D	Oui
Notifications pour Microsoft 365, Google Workspace et les autres sauvegardes basées sur le Cloud	N/D	Oui

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.

Remarque

Tous les terminaux associés à l'utilisateur désactivé ne seront plus protégés car aucun quota ne leur sera appliqué. Pour continuer la protection de ces terminaux, réaffectez-les à un utilisateur actif.

Pour réactiver un compte utilisateur désactivé

1. Dans le portail de gestion, accédez à **Utilisateurs**.
2. Sélectionnez l'utilisateur désactivé dans la liste des utilisateurs, puis cliquez sur l'icône de points de suspension  > **Activer**.

Suppression d'un compte utilisateur

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

Remarque

Vous pouvez réutiliser le nom d'utilisateur d'un utilisateur que vous avez supprimé.

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](#) ».

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 :

- Toutes les notifications configurées pour ce compte seront désactivées.
- Toutes les données appartenant à ce compte utilisateur seront supprimées.
- L'administrateur n'aura pas accès au portail de gestion.
- Toutes les sauvegardes des ressources associées à cet utilisateur seront supprimées.
- Toutes les machines associées à ce compte utilisateur seront désenregistrées.
- Tous les plans de protection seront révoqués pour toutes les ressources associées à cet utilisateur.
- Toutes les données File Sync & Share appartenant à cet utilisateur (par exemple, les fichiers et les dossiers) seront supprimées.
- Les données de Notary appartenant à cet utilisateur (par exemple, les fichiers notariés, les fichiers signés électroniquement) seront supprimées.
- L'**état** de l'utilisateur indique **Supprimé**. Lorsque vous survolez l'état **Supprimé**, la date de suppression de l'utilisateur apparaît, ainsi qu'une remarque indiquant que vous pouvez toujours restaurer tous les paramètres et données de l'utilisateur pertinents dans les 30 jours suivant la date de leur suppression.

Transférer la propriété d'un compte utilisateur

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

Important

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

Pour transférer la propriété d'un compte utilisateur :

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

6. Sélectionnez le compte utilisateur dont vous transférez la propriété, puis cliquez sur l'icône en forme de points de suspension  > **Réinitialiser le mot de passe.**
7. Confirmez votre action en cliquant sur **Réinitialiser.**
8. Laissez le futur propriétaire du compte réinitialiser le mot de passe en suivant les instructions qui lui seront envoyées par e-mail.

Le nouveau propriétaire peut désormais accéder à ce compte.

Configurer l'authentification à deux facteurs

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

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

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

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

Remarque

Pour les tenants partenaires en mode production, l'authentification à deux facteurs est activée par défaut et ne peut pas être désactivée.

Pour les tenants clients, l'authentification à deux facteurs est facultative et peut être désactivée.

Fonctionnement

1. Vous **activez l'authentification à deux facteurs** au niveau de votre organisation.
2. Tous les utilisateurs de l'organisation doivent installer une application d'authentification sur le terminal qui applique le second facteur (téléphone mobile, ordinateur portable ou de bureau, ou tablette). Cette application sera utilisée pour générer des codes TOTP uniques. Les authentificateurs recommandés sont les suivants :
 - Google Authenticator
Version de l'application iOS (<https://apps.apple.com/app/google-authenticator/id388497605>)

Version Android

(<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>)

- Microsoft Authenticator

Version de l'application iOS (<https://apps.apple.com/app/microsoft-authenticator/id983156458>)

Version Android (<https://play.google.com/store/apps/details?id=com.azure.authenticator>)

Important

Les utilisateurs doivent s'assurer que l'heure indiquée sur le terminal 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 de 32 chiffres indiqué en dessous du QR code et l'ajouter manuellement dans l'application d'authentification.

Important

Il est vivement recommandé de l'enregistrer (imprimez le QR code, notez le mot de passe temporaire à usage unique (TOTP), utilisez l'application prenant en charge la sauvegarde de codes dans un cloud). Vous aurez besoin du mot de passe temporaire à usage unique (TOTP) pour réinitialiser l'authentification à deux facteurs si vous perdez le terminal qui applique le second facteur.

6. Le mot de passe temporaire à usage unique (TOTP) sera généré dans l'application d'authentification. Il est automatiquement régénéré toutes les 30 secondes.
7. Dans la fenêtre **Configurer l'authentification à deux facteurs**, les utilisateurs doivent saisir le mot de passe temporaire à usage unique 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.

Pour restaurer l'authentification à deux facteurs sur un nouveau terminal

Si vous avez accès à l'application d'authentification sur mobile configurée précédemment :

1. Installez une application d'authentification sur votre nouveau terminal.
2. Utilisez le fichier PDF que vous avez enregistré lorsque vous avez configuré l'authentification à deux facteurs sur votre terminal. Ce fichier contient le code à 32 chiffres qui doit être saisi dans l'application d'authentification pour réassocier cette application à votre compte Acronis.

Important

Si le code est correct, mais ne fonctionne pas, veuillez à synchroniser l'heure dans l'application d'authentification pour mobile.

3. Si vous n'avez pas enregistré le fichier PDF pendant l'installation :
 - a. Cliquez sur **Réinitialiser l'authentification à deux facteurs** et saisissez le mot de passe à usage unique dans l'application d'authentification sur mobile configurée précédemment.
 - b. Suivez les instructions affichées à l'écran.

Si vous n'avez pas accès à l'application d'authentification sur mobile configurée précédemment :

1. Prenez un nouveau terminal mobile.
2. Utilisez le fichier PDF stocké pour associer un nouveau terminal (le nom par défaut du fichier est `cyberprotect-2fa-backupcode.pdf`).
3. Restaurez l'accès à votre compte depuis la sauvegarde. Assurez-vous que les sauvegardes sont prises en charge par votre application mobile.
4. Ouvrez l'application dans le même compte, depuis un autre terminal mobile s'il est pris en charge par l'application.

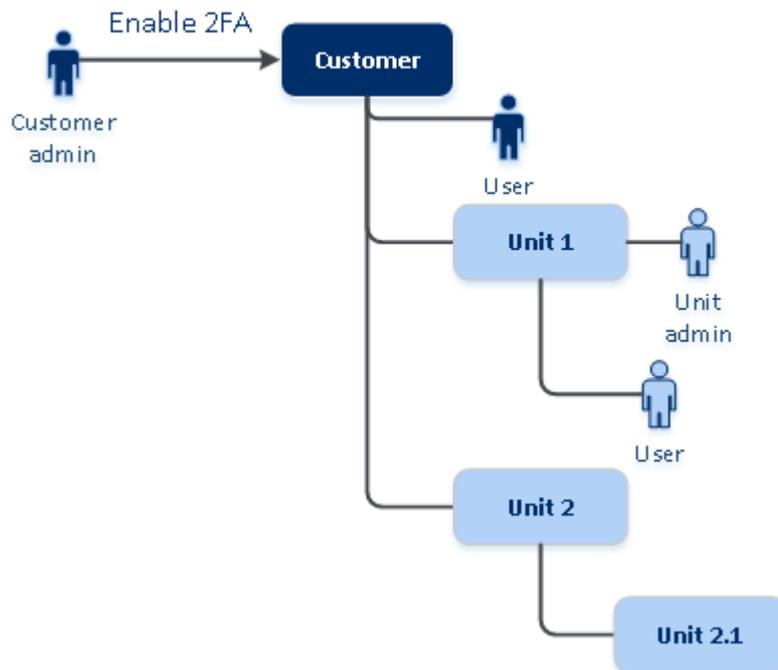
Propagation de la configuration de l'authentification à deux facteurs à tous les niveaux de tenants

L'authentification à deux facteurs est définie au niveau de l'**organisation**. Vous pouvez configurer l'authentification à deux facteurs pour votre propre organisation uniquement.

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

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

2FA setting propagation from a customer level



Remarque

1. Il n'est pas possible de configurer l'authentification à deux facteurs au niveau de l'unité.
2. Vous pouvez gérer les paramètres de l'authentification à deux facteurs pour les utilisateurs des organisations enfants (unités).

Configuration de l'authentification à deux facteurs pour vos tenants

En tant qu'administrateur d'entreprise, vous pouvez activer l'authentification à deux facteurs pour les utilisateurs de votre organisation.

Pour activer l'authentification à deux facteurs

Rôle requis : administrateur d'entreprise

1. Connectez-vous au portail de gestion.
2. Accédez à **Paramètres** > **Sécurité**.
3. Faites glisser le commutateur **Authentification à deux facteurs**, puis cliquez sur **Activer**.

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

La barre de progression sous le commutateur affiche le nombre d'utilisateurs ayant configuré l'authentification à deux facteurs pour leur compte. Pour vérifier quels utilisateurs ont configuré leur compte, accédez à **Mon entreprise** > onglet **Utilisateurs**, puis consultez la colonne

Statut 2FA. Le statut 2FA (authentification à deux facteurs) des utilisateurs qui n'ont pas encore configuré ce type d'authentification pour leur compte est **Configuration requise**.

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

Pour désactiver l'authentification à 2 facteurs

Rôle requis : administrateur d'entreprise

1. Connectez-vous au portail de gestion.
2. Accédez à **Paramètres > Sécurité**.
3. Pour désactiver l'authentification à deux facteurs, désactivez le commutateur, puis cliquez sur **Désactiver**.
4. [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.

L'authentification à deux facteurs est désactivée pour l'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 **Mon entreprise > onglet Utilisateurs**, la colonne **Statut 2FA** est masquée.

Gestion de l'authentification à 2 facteurs pour les utilisateurs

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

Surveillance

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

Pour réinitialiser l'authentification à deux facteurs pour un utilisateur

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

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

Pour réinitialiser les navigateurs fiables pour un utilisateur

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

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

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

Pour désactiver l'authentification à deux facteurs pour un utilisateur

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

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

Important

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

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

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

4. [Si au moins un utilisateur au sein d'un tenant a configuré l'authentification à deux facteurs]
Pour confirmer la désactivation, saisissez le code TOTP généré dans l'application d'authentification du terminal qui applique le second facteur.

Pour activer l'authentification à deux facteurs pour un utilisateur

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

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

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

Pour réinitialiser l'accès à votre compte en cas de perte du terminal 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 terminal appliquant le second facteur et ajoutez le code secret TOTP dans l'application d'authentification installé sur ce terminal.
- Demandez à votre administrateur [de réinitialiser les paramètres de l'authentification à deux facteurs pour vous](#).

Protection contre les attaques en force brute

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

Le mécanisme de protection contre les attaques en force brute de la plateforme est basé sur les [cookies de terminal](#).

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 terminal 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 terminal 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 terminal. Cela signifie que si un utilisateur tente de saisir le code TOTP à l'aide de différents terminaux, il sera bloqué.

Configuration des mises à jour de l'agent Cyber Protection

Important

Vous pouvez accéder à la fonctionnalité de gestion de la mise à jour de l'agent si vous avez activé le service Protection.

Cette procédure s'applique aux mises à jour des agents Cyber Protection suivants : agent pour Windows, agent pour Linux, agent pour Mac et Cloud Cyber Files agent pour File Sync & Share.

Cloud Cyber Files possède une version de l'agent de bureau File Sync & Share pour Windows et une autre pour macOS, qui permet la synchronisation de fichiers et de dossiers entre un ordinateur et la zone de stockage dans le cloud File Sync & Share d'un utilisateur afin de promouvoir le travail hors ligne, ainsi que le télétravail et les pratiques BYOD (Bring Your Own Device - Apporter votre propre terminal).

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

Remarque

Pour gérer les agents sur des machines individuelles et personnaliser les paramètres de mise à jour automatique depuis la console Cyber Protect, voir la section [Mise à jour des agents](#) dans le [Cyber Protect Guide de l'utilisateur](#).

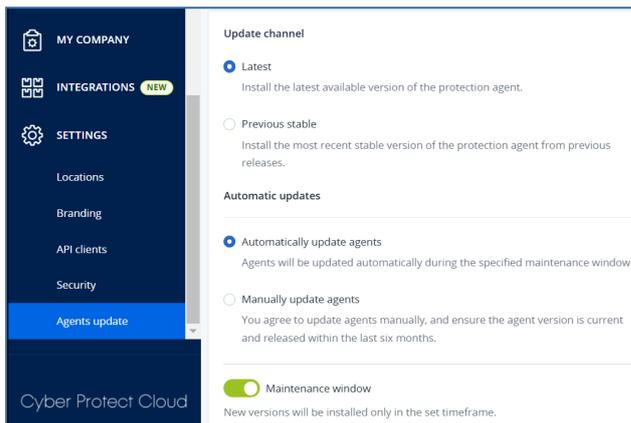
Mises à jour automatiques

Remarque

Si vous n'avez pas activé le service Protection, les paramètres de mises à jour automatiques de l'agent pour File Sync & Share sont hérités de votre fournisseur de services.

Pour configurer les paramètres par défaut des mises à jour automatiques des agents dans le portail de gestion

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



2. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

3. Vérifiez que l'option **Mettre à jour automatiquement les agents** est activée.

Remarque

Les mises à jour automatiques ne sont disponibles que pour les agents suivants :

- Agent Cyber Protect version 26986 (publiée en mai 2021) ou versions ultérieures.
- L'agent de bureau File Sync & Share version 15.0.30370 et versions ultérieures.

Les agents plus anciens doivent d'abord être mis à jour vers la dernière version avant que les mises à jour automatiques entrent en vigueur.

4. [Facultatif] Définissez la fenêtre de maintenance.

La fenêtre par défaut est quotidienne, de 23 h 00 à 8 h 00, sur la machine où l'agent est installé.

Remarque

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

5. Cliquez sur **Enregistrer**.

Mises à jour manuelles**Important**

Nous vous recommandons vivement d'activer les mises à jour automatiques pour vos agents. Grâce aux mises à jour régulières, vous tenez vos agents à jour, obtenez de meilleures performances, corrigez les problèmes de bogues, et améliorez les fonctionnalités de protection et de sécurité.

Pour configurer les paramètres par défaut pour les mises à jour manuelles des agents dans le portail de gestion

1. Accédez à **Paramètres > Mise à jour des agents**.
2. Sous **Canal de mise à jour**, sélectionnez la version à utiliser pour les mises à jour automatiques.

Option	Description
Dernière (sélectionné par défaut)	Installez la dernière version disponible de l'agent Cyber Protection.
Précédente version stable	Parmi les versions précédentes, installez la dernière version stable de l'agent Cyber Protection.

3. Sélectionnez **Mettre à jour les agents manuellement**.

The screenshot shows a configuration window with the following sections:

- Update channel**
 - Latest: Install the latest available version of the protection agent.
 - Previous stable: Install the most recent stable version of the protection agent from previous releases.
- Automatic updates**
 - Automatically update agents: Agents will be updated automatically during the specified maintenance window.
 - Manually update agents: You agree to update agents manually, and ensure the agent version is current and released within the last six months.
 - Enforce automatic updates for unsupported versions: Agents older than 6 months will be updated automatically during the specified maintenance window.
- Maintenance window**
 - Maintenance window: New versions will be installed only in the set timeframe.

At the bottom, there are input fields for 'From' and 'To' times.

4. [Facultatif] Pour éviter les risques de sécurité, garantir l'accès aux dernières fonctionnalités et minimiser les problèmes techniques causés par des agents très obsolètes, activez les mises à jour automatiques des agents de plus de 6 mois.
 - a. Sélectionnez **Appliquer les mises à jour automatiques des versions non prises en charge**.

Important

Si vous n'avez pas activé les mises à jour automatiques des agents avant de passer à la version C25.02, cette option est activée automatiquement pour tous les tenants de votre environnement.

- b. [Facultatif] Définissez la fenêtre de maintenance.

La fenêtre de maintenance par défaut est quotidienne, de 23h00 à 8h00, sur la machine où l'agent est installé.

Remarque

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

5. Cliquez sur **Enregistrer**.

Surveillance des mises à jour de l'agent

Important

Les mises à jour des agents ne peuvent être surveillées que si vous avez activé le module Protection.

Pour surveiller les mises à jour des agents, voir les sections [Alertes](#) et [Activités](#) du [Cyber Protect Guide de l'utilisateur](#).

Stockage immuable

Le stockage immuable est un type de stockage de données qui empêche la modification, l'altération ou la suppression des sauvegardes pendant une période définie. Il garantit que les données restent sécurisées et inviolables en fournissant une couche de protection supplémentaire contre les modifications non autorisées et involontaires, ainsi que les attaques de ransomware. Le stockage immuable est disponible pour toutes les sauvegardes stockées dans une instance de stockage cloud prise en charge. Voir "Stockages et agents pris en charge" (p. 47).

Grâce au stockage immuable, vous pouvez accéder à des sauvegardes supprimées pendant la période de rétention spécifiée. Vous pouvez restaurer des contenus depuis ces sauvegardes, mais vous ne pouvez ni les modifier, ni les déplacer, ni les supprimer. À la fin de la période de rétention, les sauvegardes supprimées sont définitivement supprimées.

Le stockage immuable contient les sauvegardes suivantes :

- Sauvegardes supprimées manuellement.
- Sauvegardes supprimées automatiquement, conformément aux paramètres de la section **Durée de conservation** d'un plan de protection ou de la section **Règles de rétention** d'un plan de nettoyage.

Les sauvegardes supprimées du stockage immuable utilisent toujours de l'espace de stockage et sont facturées en conséquence.

Les tenants supprimés ne sont facturés pour aucun stockage, pas même le stockage immuable.

Modes de stockage immuable

Un administrateur client peut désactiver et réactiver le stockage immuable, et modifier son mode et sa période de rétention.

Le stockage immuable est disponible dans les modes suivants :

- **Mode de gouvernance**

Vous pouvez désactiver et réactiver le stockage immuable. Vous pouvez modifier la période de rétention ou passer en mode de conformité.

Remarque

À partir de septembre 2024, le mode de gouvernance du stockage immuable avec une période de rétention de 14 jours peut être activé automatiquement pour votre entreprise. Consultez votre fournisseur de services pour plus de détails.

- **Mode de conformité**

Avertissement !

La sélection du mode de conformité est irréversible.

Vous ne pouvez pas désactiver le stockage immuable. Vous ne pouvez pas modifier la période de rétention ni revenir au mode de gouvernance.

Stockages et agents pris en charge

- Le stockage immuable n'est pris en charge que pour le stockage dans le cloud.
 - Le stockage immuable est disponible pour les stockages cloud hébergés par Acronis et par les partenaires utilisant Cyber Infrastructure version 4.7.1 ou ultérieure.
 - Tous les systèmes de stockage pouvant être utilisés avec Cyber Infrastructure Backup Gateway sont pris en charge. Par exemple, le stockage Cyber Infrastructure, les stockages Amazon S3 et EC2, et le stockage Microsoft Azure.
 - Le stockage immuable nécessite que le port TCP 40440 soit ouvert pour le service Backup Gateway dans Cyber Infrastructure. Dans les versions 4.7.1 et ultérieure, le port TCP 40440 est automatiquement ouvert avec le type de trafic **public Backup (ABGW)**. Pour plus d'informations sur les types de trafic, consultez la [documentation d'Acronis Cyber Infrastructure](#).
- Le stockage immuable nécessite un agent de protection version 21.12 (15.0.28532) ou ultérieure.
- Seules les sauvegardes TIBX (version 12) sont prises en charge.

Configuration d'un stockage immuable

Après septembre 2024, le mode de gouvernance du stockage immuable, avec une période de rétention de 14 jours, est activé par défaut. Vous pouvez modifier les paramètres par défaut de

votre organisation, si nécessaire.

Remarque

Pour permettre l'accès aux sauvegardes supprimées, le port 40440 sur le stockage des sauvegardes doit être activé pour les connexions entrantes.

Pour modifier la période de rétention ou le mode de stockage immuable

1. Connectez-vous au portail de gestion en tant qu'administrateur, puis accédez à **Paramètres > Sécurité**.

2. Vérifiez que le commutateur **Stockage immuable** est activé.

3. Spécifiez une période de rétention comprise entre 14 et 3 650 jours.

Par défaut, la période de rétention est de 14 jours. Une période de rétention plus longue augmentera l'utilisation du stockage.

4. Sélectionnez le mode de stockage immuable et, si vous y êtes invité, confirmez votre choix.

- **Mode de gouvernance**

Ce mode garantit que les ransomware ou les acteurs malveillants ne peuvent pas altérer ni effacer les données de sauvegarde, car toutes les sauvegardes supprimées sont conservées dans le stockage immuable pendant la période de rétention que vous avez spécifiée. Il garantit également l'intégrité des données de sauvegarde, ce qui est essentiel pour la reprise d'activité après sinistre.

Vous pouvez désactiver et réactiver le stockage immuable, modifier la période de rétention ou passer en mode de conformité.

- **Mode de conformité**

Outre les avantages du mode de gouvernance, le mode de conformité aide les organisations à respecter les exigences réglementaires en matière de rétention et de sécurité des données en empêchant toute altération des données.

Avertissement !

Le choix du mode de conformité est irréversible. Après avoir sélectionné ce mode, vous ne pouvez ni désactiver le stockage immuable, ni modifier la période de rétention, ni revenir au mode de gouvernance.

5. Cliquez sur **Enregistrer**.

Avertissement !

La sélection du **Mode de conformité** est irréversible. Après avoir sélectionné ce mode, vous ne serez plus autorisé à désactiver le stockage immuable, ni à modifier son mode ou sa période de rétention.

6. Pour ajouter une archive existante au stockage non modifiable, créez une nouvelle sauvegarde dans cette archive en exécutant le plan de protection correspondant manuellement ou sur un calendrier.

Avertissement !

Si vous supprimez une sauvegarde avant d'ajouter l'archive au stockage immuable, elle est supprimée définitivement.

Pour désactiver le stockage immuable

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

Remarque

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

Avertissement !

La désactivation du stockage immuable n'est pas immédiate. Pendant une période de grâce de 14 jours (336 heures), vous pouvez accéder aux sauvegardes supprimées en fonction de leur période de rétention d'origine.

Lorsque la période de grâce se termine, toutes les sauvegardes dans le stockage immuable sont définitivement supprimées. Par exemple, si vous désactivez le stockage immuable le 1er octobre à 10 h 00, toutes les sauvegardes qui sont encore dans le stockage immuable le 15 octobre à 10 h 00 seront définitivement supprimées.

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

Affichage de l'utilisation du stockage immuable

Vous pouvez consulter l'espace utilisé par le stockage immuable dans la console Cyber Protect ou dans le rapport **Utilisation actuelle** que vous pouvez générer depuis le Portail de gestion.

Limites

- La valeur indiquée comprend la taille totale de toutes les sauvegardes supprimées, ainsi que les métadonnées des archives de sauvegarde dans le stockage. Les métadonnées peuvent représenter jusqu'à 10 % de la valeur indiquée.
- La valeur indique l'utilisation jusqu'à 24 heures avant la génération du rapport.
- Si l'utilisation réelle est inférieure à 0,01 Go, elle est affichée sous la forme 0,0 Go.

Pour afficher l'utilisation du stockage immuable

Dans la console Cyber Protect

1. Connectez-vous à la console Cyber Protect.
2. Accédez à **Stockage des sauvegardes > Sauvegardes**, puis sélectionnez un emplacement de stockage dans le cloud qui prend en charge le stockage immuable.
3. Vérifiez la colonne **Stockage immuable et métadonnées**.

Dans le rapport Utilisation actuelle

1. Connectez-vous au portail de gestion en tant qu'administrateur.
2. Accédez à **Rapports > Utilisation**.
3. Sélectionnez **Utilisation actuelle**, puis cliquez sur **Générer et envoyer**.
Un rapport aux formats CSV et HTML est envoyé à votre adresse e-mail.
Le fichier HTML est inclus dans une archive ZIP.
4. Dans le rapport, vérifiez la colonne **Nom de l'indicateur**.
Vous pouvez voir l'utilisation du stockage immuable dans la ligne **Stockage dans le cloud - Immuable**.

Exemple de facturation pour le stockage immuable

L'exemple ci-dessous représente une sauvegarde supprimée qui aboutit au stockage immuable pendant 14 jours, ce qui correspond à la période de rétention par défaut. Pendant cette période, la sauvegarde supprimée utilise de l'espace de stockage. À la fin de la période de rétention, la sauvegarde supprimée est définitivement supprimée et l'utilisation du stockage diminue. Tous les mois, l'utilisation du stockage est facturée en conséquence.

Date	Sauvegardes	Utilisation du stockage	Facturation
1er avril	La sauvegarde A (10 Go) est créée La sauvegarde B (1 Go) est créée	10 Go + 1 Go = 11 Go	
20 avril	La sauvegarde B est supprimée, aboutit au stockage immuable (avec une période de rétention de 14 jours)	10 Go + 1 Go = 11 Go	
30 avril			Facturation de 11 Go pour avril
4 mai	La sauvegarde B est supprimée définitivement, car la période de rétention est terminée	11 Go - 1 Go = 10 Go	
31 mai			Facturation de 10 Go pour mai

Activation de la formation avancée de sensibilisation à la sécurité pour les utilisateurs de votre organisation

La formation de sensibilisation à la sécurité est fournie par le fournisseur tiers Wizer en tant qu'intégration dans la console Cyber Protect Cloud. Si votre fournisseur de services a activé le service pour votre organisation, vous devez activer l'intégration afin de permettre à vos utilisateurs d'accéder aux supports de formation.

Pour activer l'intégration avec Wizer pour une organisation

Rôle requis : Administrateur client, administrateur de la protection ou cyberadministrateur.

Remarque

Cette configuration initiale est effectuée une seule fois.

1. Connectez-vous à la console Cyber Protect Cloud.
2. Dans le menu de navigation, cliquez sur **Formation de sensibilisation à la sécurité > Tableau de bord de la sensibilisation**.
3. Cliquez sur **Activer l'intégration**.
4. Cliquez sur **Activer** pour confirmer.

Une fois l'intégration activée, un nouveau tenant est provisionné pour l'organisation dans la plateforme Wizer. Si vous avez déjà un compte sur Wizer et souhaitez l'utiliser au lieu d'utiliser un nouveau tenant, contactez votre fournisseur de services.

Vous pouvez accéder au panneau d'administration Wizer et ajouter des utilisateurs manuellement en important un fichier CSV ou en configurant l'authentification unique avec Active Directory, Octa, Google ou un autre fournisseur d'identité. Voir [Comment ajouter des utilisateurs](#).

Limitation de l'accès à l'interface Web

Vous pouvez limiter l'accès à l'interface Web en spécifiant une liste d'adresses IP à partir desquelles les utilisateurs sont autorisés à se connecter.

Remarque

Cette restriction s'applique également à l'accès au portail de gestion via l'[API](#).

Remarque

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

Pour limiter l'accès à l'interface Web

1. Connectez-vous au portail de gestion.
2. [Naviguez vers l'unité](#) à laquelle vous souhaitez limiter l'accès.
3. Cliquez sur **Paramètres > Sécurité**.
4. Sélectionnez la case à cocher **Activer le 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**.

Limitez l'accès à votre société

Vous pouvez limiter l'accès des administrateurs de niveau supérieur à votre entreprise.

En tant qu'administrateur du portail de gestion, si vous limitez l'accès à votre entreprise, les administrateurs de votre partenaire fournisseur de services ne pourront que modifier les propriétés et les quotas de votre entreprise, et obtenir des rapports d'utilisation pour votre entreprise et pour vos clients. Ils ne pourront pas accéder aux informations suivantes :

- Informations figurant dans votre tenant.
- Vos clients, leurs utilisateurs, services, sauvegardes, et autres ressources.

Pour limiter l'accès à votre entreprise

1. Connectez-vous au portail de gestion.
2. Cliquez sur **Paramètres > Sécurité**.
3. Désactivez l'option **Accès à l'assistance**.

Gestion des tâches

Si votre compte comprend l'accès au service Advanced Automation (PSA), cliquez sur **Gestion des tâches** pour afficher et gérer vos tickets auprès du service d'assistance.

Remarque

Les utilisateurs auxquels le rôle Gestionnaire des clients a été attribué dans Advanced Automation (PSA) peuvent voir et gérer tous les tickets du service d'assistance dans l'organisation ; ceux ayant le rôle Client ne peuvent voir et mettre à jour que leurs propres tickets.

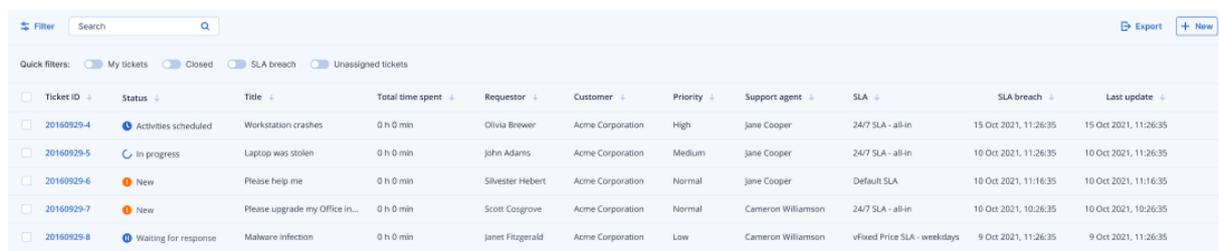
Affichage des tickets auprès du service d'assistance

Pour afficher les tickets existants du service d'assistance, accédez depuis le portail de gestion à **Gestion des tâches > Service d'assistance**. Les informations concernant chaque ticket sont affichées :

- Lien vers le ticket.
- Statut actuel du ticket.
- Total du temps passé sur le ticket.
- Utilisateur ayant fait la demande de ticket.
- Client.
- Priorité du ticket.
- Agent du support affecté.
- Accord de niveau de service (SLA) attribué, moment de violation de cet accord et prochaine mise à jour prévue de la part d'un ingénieur dédié.
- Date de dernière mise à jour du ticket.

Pour exporter des données de tickets, cliquez sur **Exporter**. Un fichier XLS intitulé **Tickets** est téléchargé sur votre ressource.

Vous pouvez également filtrer et trier la liste qui s'affiche pour retrouver un ticket spécifique ; si vous souhaitez un filtrage plus précis, utilisez l'outil **Filtrer** pour définir les tickets à afficher.



Ticket ID	Status	Title	Total time spent	Requestor	Customer	Priority	Support agent	SLA	SLA breach	Last update
20160929-4	Activities scheduled	Workstation crashes	0 h 0 min	Olivia Brewer	Acme Corporation	High	Jane Cooper	24/7 SLA - all-in	15 Oct 2021, 11:26:35	15 Oct 2021, 11:26:35
20160929-5	In progress	Laptop was stolen	0 h 0 min	John Adams	Acme Corporation	Medium	Jane Cooper	24/7 SLA - all-in	10 Oct 2021, 11:26:35	10 Oct 2021, 11:26:35
20160929-6	New	Please help me	0 h 0 min	Silvester Hebert	Acme Corporation	Normal	Jane Cooper	Default SLA	10 Oct 2021, 11:16:35	10 Oct 2021, 11:16:35
20160929-7	New	Please upgrade my Office in...	0 h 0 min	Scott Cosgrove	Acme Corporation	Normal	Cameron Williamson	24/7 SLA - all-in	10 Oct 2021, 10:26:35	10 Oct 2021, 10:26:35
20160929-8	Waiting for response	Malware infection	0 h 0 min	James Fitzgerald	Acme Corporation	Low	Cameron Williamson	vFixed Price SLA - weekdays	9 Oct 2021, 11:26:35	9 Oct 2021, 11:26:35

Création d'un ticket auprès du service d'assistance

Pour créer un nouveau ticket

1. Accédez à **Gestion des tâches > Service d'assistance**. La liste des tickets ouverts s'affiche.

Remarque

Les utilisateurs auxquels le rôle Gestionnaire des clients a été attribué dans Advanced Automation (PSA) voient tous les tickets du service d'assistance dans l'organisation ; ceux ayant le rôle Client ne voient que leurs propres tickets.

2. Cliquez sur **+ Nouveau**. La boîte de dialogue Créer un nouveau ticket s'affiche.
3. Définissez ce qui suit :
 - Dans le champ **Titre du ticket**, ajoutez le titre du ticket.
 - Dans le champ **Demandeur** (activé uniquement pour les utilisateurs ayant le rôle Gestionnaire des clients), sélectionnez l'utilisateur souhaité dans la liste des contacts et utilisateurs actifs du client. Notez que le champ **Nom du client** est désactivé pour les utilisateurs Gestionnaire des clients et Client.
 - (Facultatif) Dans le champ **Numéro de téléphone**, ajoutez un numéro de téléphone. Notez que, si vous mettez à jour le numéro par défaut, le nouveau numéro est stocké en tant que numéro de téléphone par défaut de l'utilisateur.
 - Dans le champ **Supérieur**, sélectionnez l'utilisateur souhaité dans la liste des utilisateurs actifs du client (par exemple, les utilisateurs auxquels le rôle Gestionnaire des clients est affecté).
 - Dans la section **Élément ou service de configuration**, sélectionnez un **service géré** ou un **service informatique** :
 - **Service géré** : Cette option est sélectionnée et préremplie avec les détails nécessaires si le type de produit Service géré est disponible dans le contrat pertinent. Notez que, si le contrat ne comporte aucun type de produit de service géré, cette option est désactivée.
 - **Service informatique** : Cette option est sélectionnée et préremplie avec les détails nécessaires si le type de produit Service informatique est disponible dans le contrat pertinent. Notez que, si le contrat ne comporte aucun type de produit de service informatique, cette option est désactivée.
 - Le champ **Élément de configuration** indique les terminaux associés au service géré ou informatique sélectionné (le message **Élément de configuration inconnu** est affiché si le terminal est inconnu) ; la sélection d'un terminal après celle d'un service est facultative (lorsque vous sélectionnez un terminal dans ce scénario, l'accord de niveau de service (SLA) ne change pas ; il reste l'accord de niveau de service (SLA) qui appartient au service).

Remarque

Les terminaux répertoriés comprennent ceux fournis par Cyber Protect. Si Cyber Protection fournit une option de contrôle distant pour un terminal répertorié, vous pouvez vous connecter à distance depuis le ticket à l'aide du protocole RDP ou d'un client HTML5.

- Vous pouvez également sélectionner une catégorie dans le champ **Catégorie**, puis définir une priorité dans le champ **Priorité**. Le champ **Accord de niveau de service (SLA)** indique l'accord de niveau de service (SLA) passé avec votre fournisseur de services managés.

- Dans la section **Mise à jour du ticket**, vous pouvez ajouter des destinataires dans les champs **À** et **Cc**. Vous pouvez également ajouter des descriptions et des commentaires en texte enrichi (y compris des images et autres fichiers multimédias, jusqu'à 25 Mo ; les formats et types pris en charge sont répertoriés ci-dessous dans la section **Pièces jointes**) dans la zone de texte affichée. Notez que le statut du ticket est défini par défaut sur **Nouveau** et ne peut pas être modifié.
- Cliquez pour activer l'interrupteur **Envoyer un e-mail au demandeur** pour vous assurer que toutes les mises à jour de ticket seront envoyées par e-mail au demandeur. Notez que lorsque des destinataires sont également ajoutés aux champs **À** et **Cc**, les notifications ne sont envoyées qu'à ces destinataires lorsque le ticket est mis à jour, et non lorsqu'il est créé.
- Dans la section **Pièces jointes**, cliquez sur les pièces jointes nécessaires (ou utilisez le glisser-déposer) pour les ajouter.

Les pièces jointes peuvent inclure les formats et types suivants (jusqu'à un maximum de 25 Mo) :

- Média : .avi, .mp4, .mp3
- E-mails : .eml, .msg
- Images : .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
- Fichiers de document et de journal : .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
- Archives : .zip, .rar

4. Cliquez sur **Terminé**. Une fois le ticket généré, il est ajouté à la liste des tickets ouverts.

Mise à jour des tickets auprès du service d'assistance

Pour mettre à jour un ticket

1. Accédez à **Gestion des tâches > Service d'assistance**. La liste des tickets ouverts s'affiche.

Remarque

Les utilisateurs auxquels le rôle Gestionnaire des clients a été attribué dans Advanced Automation (PSA) voient tous les tickets du service d'assistance dans l'organisation ; ceux ayant le rôle Client ne voient que leurs propres tickets.

2. (Facultatif) Si vous avez un grand nombre de tickets, utilisez le filtre pour localiser le ou les tickets que vous recherchez.
Cliquez sur **Filtre** (ou **Filtres enregistrés** si vous avez déjà défini un filtre), puis sélectionnez les valeurs pertinentes dans les différents champs. Notez que vous pouvez cliquer sur l'option **Ajouter aux filtres enregistrés** pour enregistrer le filtre défini à des fins ultérieures.
Vous pouvez également utiliser la barre **Recherche** pour localiser le ou les tickets pertinents.
3. Cliquez sur le lien de la ligne de ticket approprié et apportez les modifications nécessaires dans les onglets affichés :

- **Activités** : Affiche l'activité récente sur le ticket, y compris le statut actuel et les commentaires ajoutés.

Remarque

Si vous modifiez le statut d'un ticket créé par une alerte dans la console Cyber Protect et sélectionnez **Fermé**, l'alerte est également fermée dans la console Cyber Protect.

- **Vue d'ensemble** : Affiche les paramètres généraux de ticket pouvant être modifiés ; pour plus d'informations, voir "Création d'un ticket auprès du service d'assistance" (p. 53).

Notez que vous pouvez modifier le statut du ticket dans cet onglet. Par exemple, vous pouvez mettre à jour son statut et sélectionner **En progrès** lorsque vous commencez à travailler sur ce ticket ou **Fermé** lorsque le ticket peut être clos. Vous pouvez également modifier les terminaux associés à un ticket ; par exemple, si un ticket créé n'indique pas le terminal correct, vous pouvez cliquer sur la liste déroulante **Élément de configuration** pour sélectionner le terminal adéquat.

Pour plus d'informations sur les différents champs disponibles lors de la modification d'un ticket, voir "Création d'un ticket auprès du service d'assistance" (p. 53).

4. Cliquez sur **Enregistrer**.

Notez que si l'interrupteur **Envoyer un e-mail au demandeur** est activé, un e-mail est envoyé à l'utilisateur concerné et à tous les destinataires définis dans les champs **À** et **Cc**.

Soumission de tickets de service d'assistance via le portail de tickets

Le portail de soumission de tickets permet aux clients de signaler des problèmes ou de demander une assistance en soumettant un formulaire simple et public, sans s'inscrire ou se connecter au système.

Lorsqu'il est soumis, un nouveau ticket est créé et affecté automatiquement à un agent de support du fournisseur.

Remarque

Le formulaire est activé ou désactivé par le fournisseur et peut être consulté par des utilisateurs enregistrés ou non enregistrés. Notez que le fournisseur peut également choisir de restreindre et de ne pas traiter les demandes d'utilisateurs non enregistrés.

Pour soumettre un ticket via le portail public de tickets

1. Accédez à l'URL du portail de tickets public partagée par le fournisseur.
2. Dans la boîte de dialogue Créer un nouveau ticket, définissez les éléments suivants :
 - Dans le champ **Titre du ticket**, ajoutez le titre du ticket.
 - Dans le champ **Adresse e-mail**, ajoutez votre adresse e-mail.

Si l'adresse e-mail est reconnue par le système, ou si le fournisseur a choisi de ne pas restreindre les demandes des utilisateurs non enregistrés, le ticket sera créé.

Si l'adresse e-mail n'est pas reconnue et si le fournisseur a choisi de ne pas traiter les demandes des utilisateurs non enregistrés, le ticket ne sera pas créé.

- [Facultatif] Dans le champ **Numéro de téléphone**, ajoutez un numéro de téléphone.
- Dans la section **Détails du ticket**, ajoutez une description et des commentaires (y compris des images et d'autres fichiers média pour un maximum de 25 Mo ; les formats et types pris en charge sont répertoriés dans la section **Pièces jointes**) de la zone de texte.
- [Facultatif] Dans la section **Pièces jointes**, cliquez sur les pièces jointes nécessaires (ou utilisez le glisser-déposer) pour les ajouter.

Les pièces jointes peuvent inclure les formats et types suivants (jusqu'à un maximum de 25 Mo) :

- Média : .avi, .mp4, .mp3
- E-mails : .eml, .msg
- Images : .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
- Fichiers de document et de journal : .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
- Archives : .zip, .rar

3. Cliquez sur **Envoyer**.

Un message de confirmation indiquant que votre ticket a été créé s'affiche. Vous recevrez également une notification par e-mail indiquant qu'un ticket a été créé.

Surveillance

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

Utilisation

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

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

Important

Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

L'utilisation du stockage pour les ressources Microsoft 365 et Google Workspace est indiquée séparément du stockage général des sauvegardes, et est affichée dans la section **Sauvegardes Microsoft 365 et Google Workspace**.

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

Remarque

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

The screenshot shows the 'Usage' section of the Acronis Cyber Protect Cloud interface. The left sidebar contains navigation options like 'MONITORING', 'Usage', 'Operations', 'Audit log', 'UNITS', 'COMPANY MANAGEMENT', 'REPORTS', 'SETTINGS', and 'Partner Portal'. The main content area displays usage metrics for 'Advanced Email Security', 'Advanced Data Loss Prevention', and 'Location: Cloud'. A red box highlights the 'Refresh usage' button in the top right corner of the main content area.

Location: Cloud		
Total storage	Backup storage	Microsoft 365 and Google Workspace ba...
144.61 GB	143.97 GB / Unlimited GB	653.41 MB / Unlimited GB
Disaster recovery storage (Advanced)	Compute points (Advanced)	Public IP addresses (Advanced)
41.12 GB / Unlimited GB	225.39 / Unlimited	0 / Unlimited
Cloud servers (Advanced)		
3 / Unlimited		

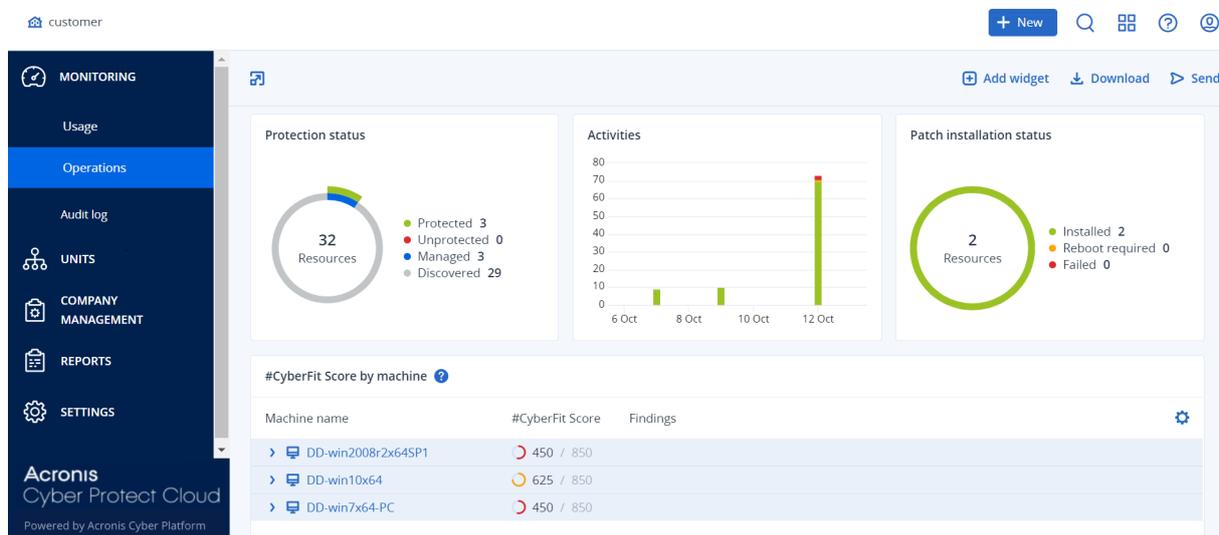
Tableau de bord des opérations

Le tableau de bord **Opérations** n'est disponible que pour les administrateurs d'entreprise lorsqu'ils travaillent à l'échelle de l'entreprise.

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.

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 ou bien l'envoyer par e-mail au format .pdf et/ou .xlsx.

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 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 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 crayon lorsque le widget est sélectionné. Lorsque vous avez terminé de modifier le widget, cliquez sur **Terminé**.

Pour supprimer un widget

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

État de protection

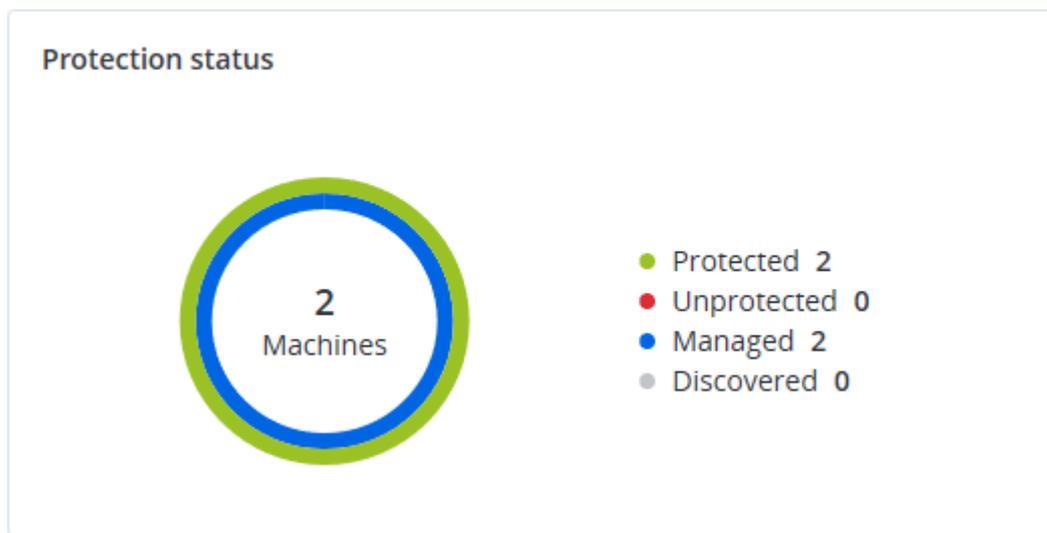
État de protection

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

Une machine peut présenter l'un des états suivants :

- **Protégé** : ordinateurs sur lesquels le plan de protection est appliqué.
- **Non protégé** : ordinateurs sur lesquels le plan de protection n'est pas appliqué. Ils comprennent à la fois les ordinateurs découverts et les ordinateurs gérés auxquels aucun plan de protection n'est appliqué.
- **Géré** : ordinateurs sur lesquels l'agent de protection est installé.
- **Découvert** : ordinateurs sur lesquels 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.



Terminaux découverts

Ce widget affiche des informations détaillées sur les terminaux qui ont été découverts dans les réseaux de l'organisation. Les informations sur les terminaux incluent le type, le fabricant, le système d'exploitation, l'adresse IP, l'adresse MAC, la date de découverte, etc.

Discovered devices										
Device name	Device type	Operating ...	Manuf...	Model	IP ad...	MAC ...	Organi... ↓	First discov...	Last discovered	Discovery type
win-2016-ad	Windows Computer	Windows	-	-	10. ...	56: ...	OU=Dom...	May 21, 20...	May 22, 2024 1...	Active Directory, Local network pas
DESKTOP-2BEV...	Windows Computer	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-J7S77IV	Windows Computer	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
acp-win2016	Unknown	-	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
win-2k19	Unknown	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
acp-virtual-mac...	Windows Computer	Windows	VMware	-	10. ...	00: ...	-	May 21, 20...	May 22, 2024 1...	Local network active, Local network
DESKTOP-8FFA...	Windows Computer	Windows	VMware	-	10. ...	00: ...	-	May 21, 20...	May 22, 2024 1...	Local network active, Local network
acp-win	Unknown	Windows	-	-	10. ...	fa: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-QCIK...	Windows Computer	Windows	-	-	10. ...	fa: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-QCIK...	Windows Computer	Windows	-	-	10. ...	fa: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive

Score #CyberFit par machine

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

- Antimalware
- Sauvegarde
- Pare-feu
- VPN
- Chiffrement
- Trafic NTLM

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

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

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

Widgets de Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) comprend un certain nombre de widgets qui sont accessibles depuis le tableau de bord **Opérations**.

Les widgets disponibles sont :

- Distribution des principaux incidents par ressource
- MTTR de l'incident
- Résolution des incidents de sécurité
- Statut réseau des ressources

Distribution des principaux incidents par ressource

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

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

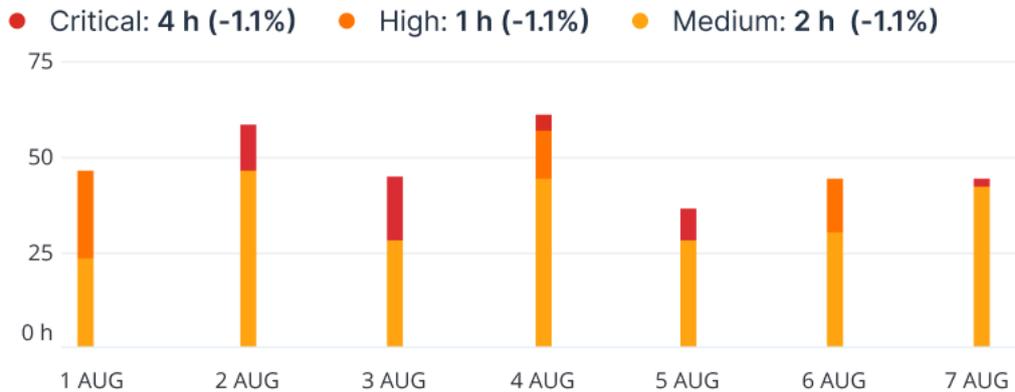


MTTR de l'incident

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

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

Incident MTTR

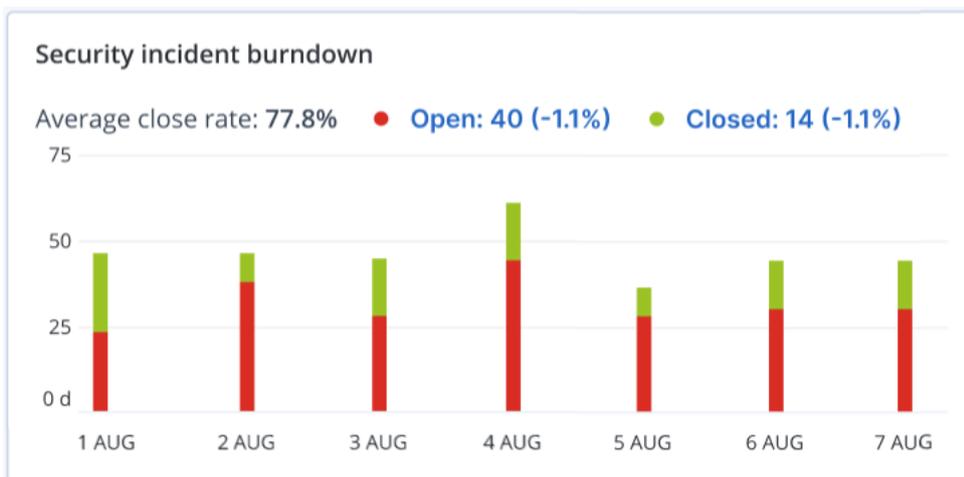


Résolution des incidents de sécurité

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

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

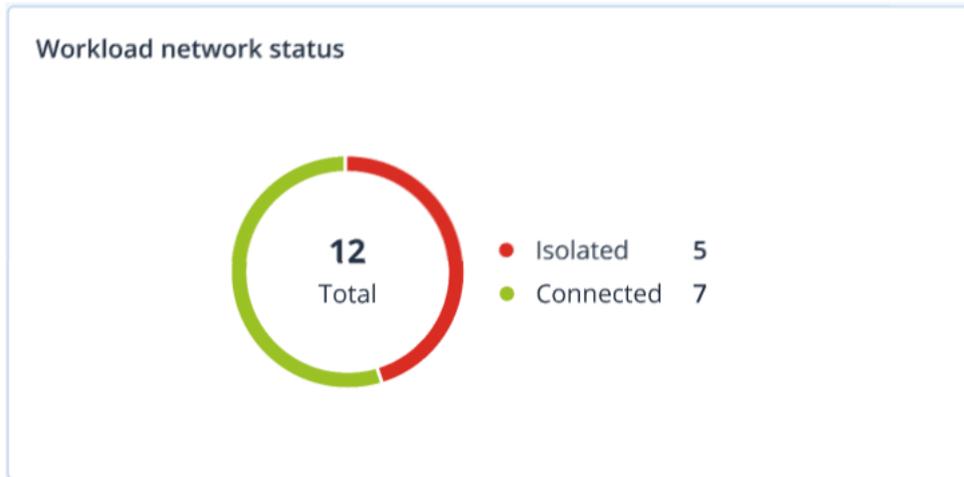
La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.



Statut réseau des ressources

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

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



Surveillance de l'intégrité du disque

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

Limites

- La prévision de l'intégrité du disque est prise en charge uniquement pour les ordinateurs Windows.
- Seuls les disques des machines physiques sont surveillés. Les disques des machines virtuelles ne peuvent pas être surveillés et ne s'affichent pas dans les widgets d'intégrité du disque.
- Les configurations RAID ne sont pas prises en charge. Les widgets d'intégrité du disque n'incluent aucune information sur les ordinateurs avec implémentation RAID.
- Les disques SSD NVMe ne sont pas supportés.
- Les terminaux de stockage externes ne sont pas pris en charge.

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

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

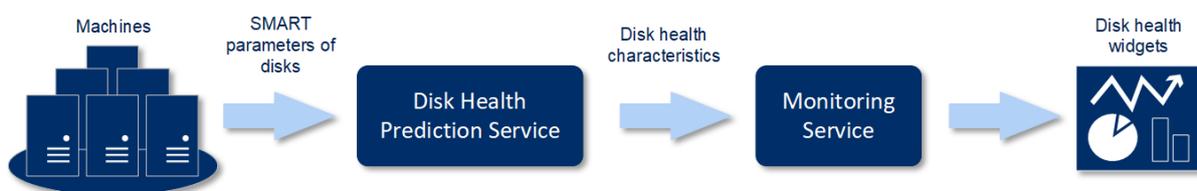
Fonctionnement

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

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

La période de prévision est d'un mois.

3. Le service de surveillance reçoit ces caractéristiques, puis affiche les informations pertinentes dans les widgets d'intégrité du disque dans la console Cyber Protect.



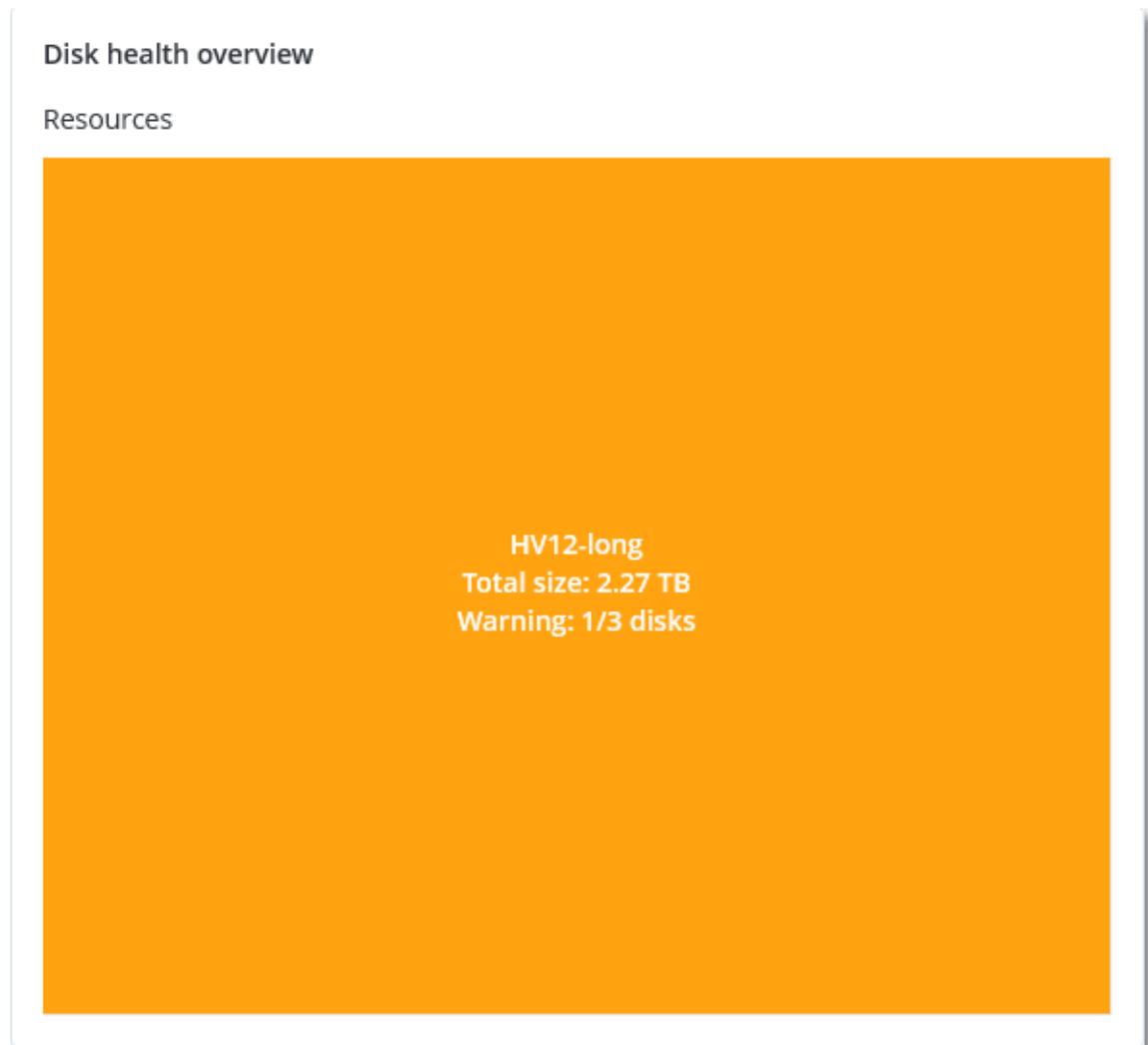
Widgets de l'état de santé du disque

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

- **Vue d'ensemble de l'intégrité du disque** est un widget en forme de carte proportionnelle, qui possède deux niveaux de détails que vous pouvez explorer :
 - Niveau ordinateur

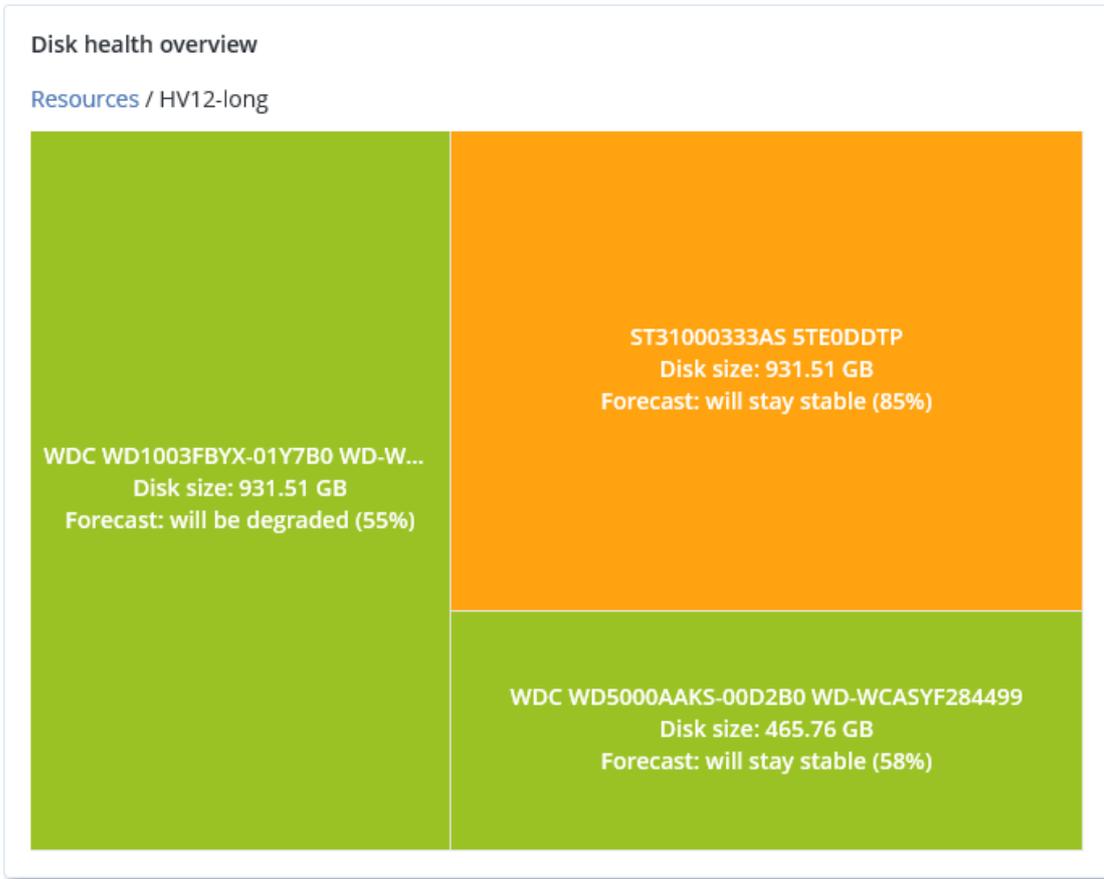
Affiche des informations résumées concernant l'intégrité du disque en fonction des ordinateurs client que vous avez sélectionnés. Seul l'état de disque le plus critique est affiché. Les autres états s'affichent dans une info-bulle lorsque vous passez le pointeur sur un bloc en particulier. La taille du bloc d'un ordinateur dépend de la taille totale de l'ensemble de ses

disques. La couleur du bloc d'une machine dépend de l'état de disque le plus critique identifié.

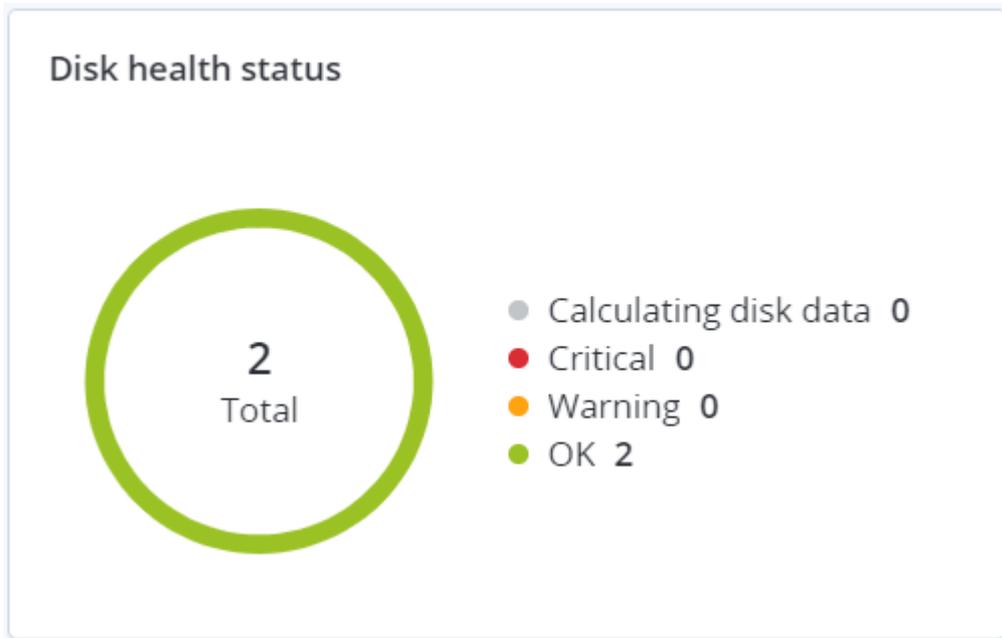


- Niveau disque
Affiche l'intégrité actuelle de tous les disques pour l'ordinateur sélectionné. Chaque bloc de disque affiche les prévisions d'intégrité du disque suivantes, ainsi que leur probabilité en pourcentage :
 - Sera altéré
 - Restera stable

- Sera amélioré



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



Alertes relatives à l'état de santé du disque

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

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

Carte de la protection des données

La fonctionnalité Carte de la protection des données vous permet de découvrir 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 forme de 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.

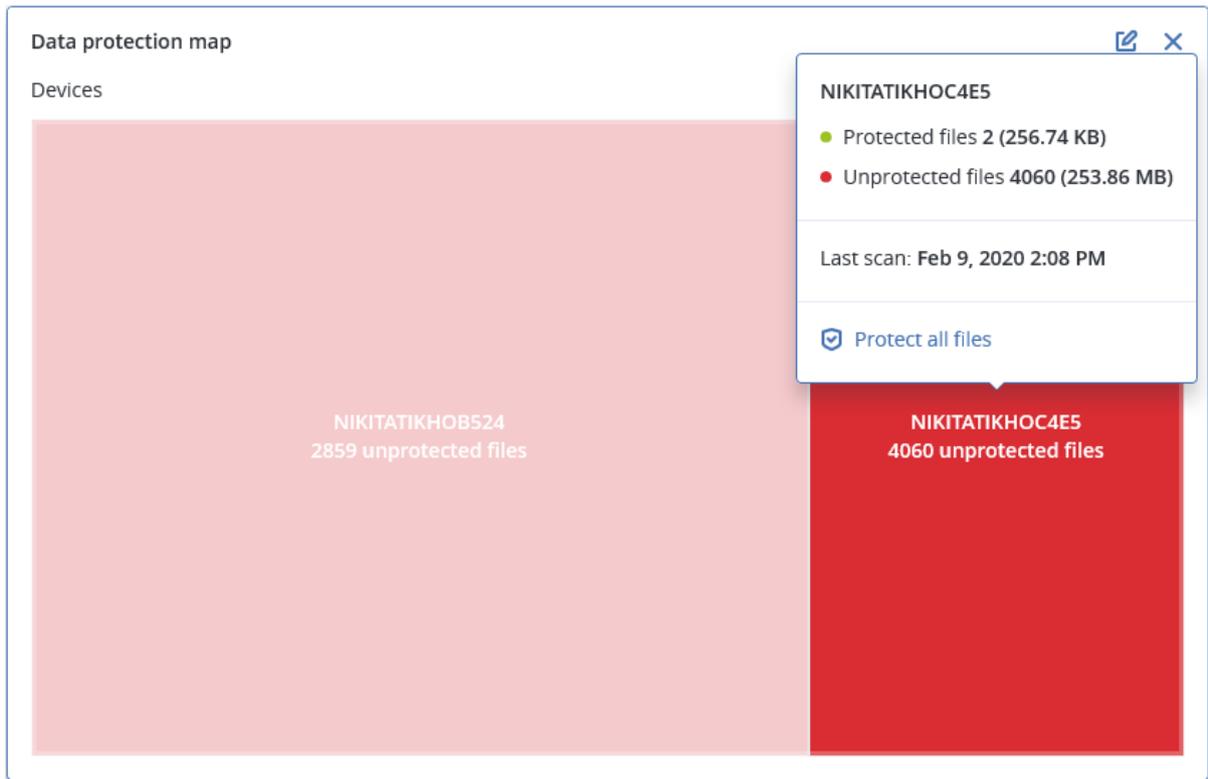
Les fichiers peuvent présenter l'un des états de protection suivants :

- **Critique** : de 51 à 100 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Basse** : de 21 à 50 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.
- **Moyen** : de 1 à 20 % des fichiers non protégés et présentant l'extension que vous avez spécifiée ne sont pas sauvegardés et ne le seront pas non plus avec les paramètres de sauvegarde existants pour la machine ou l'emplacement sélectionné.

- **Élevé** : tous les fichiers présentant l'extension que vous avez spécifiée sont protégés (sauvegardés) pour la machine ou l'emplacement 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 permet d'afficher des informations au niveau machine :

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



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

Vous pouvez aussi télécharger un rapport détaillé au format CSV.

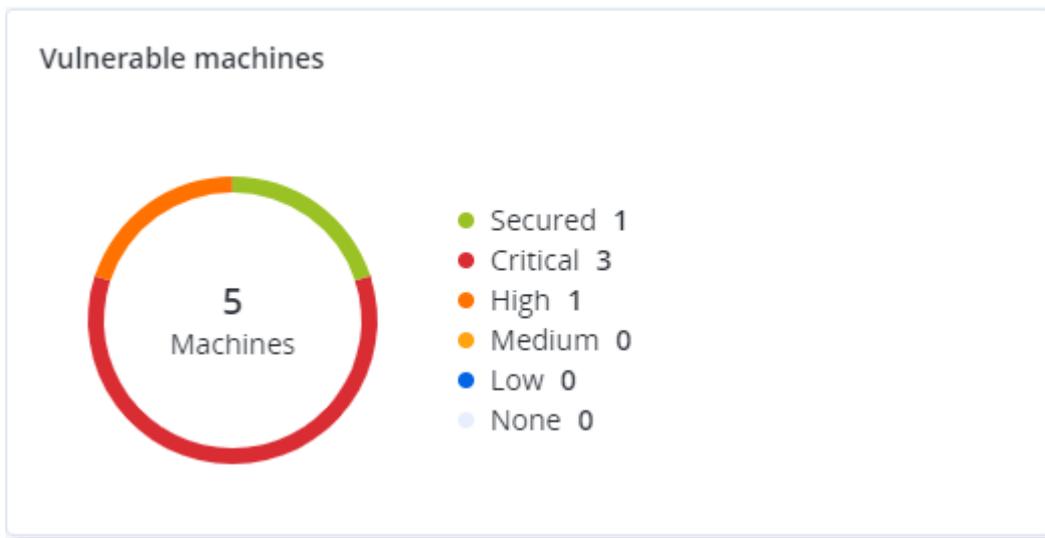
Widgets d'évaluation des vulnérabilités

Machines vulnérables

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

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

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



Vulnérabilités existantes

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

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

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

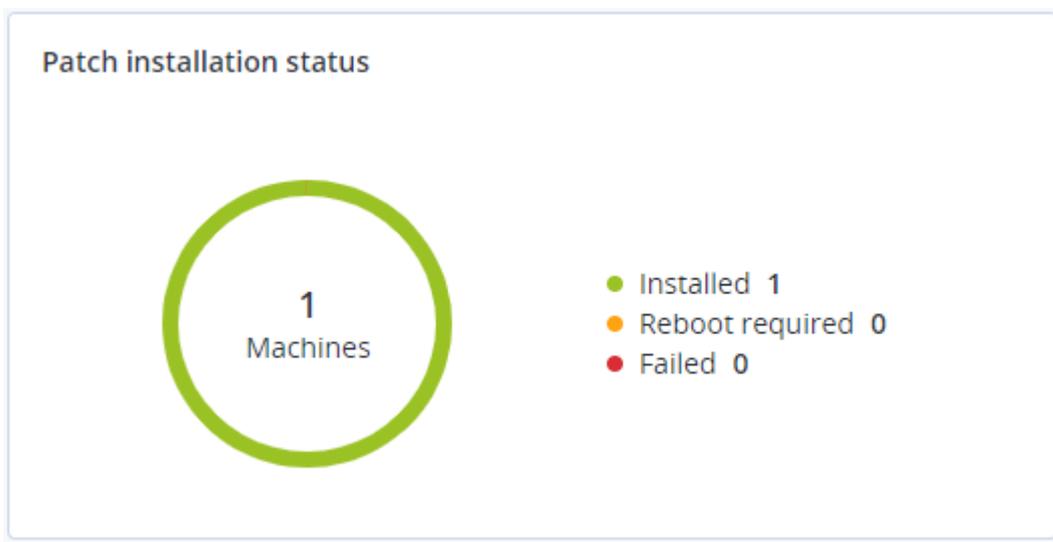
Widgets d'installation des correctifs

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

Statut d'installation des correctifs

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

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



Résumé d'installation des correctifs

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

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

Historique d'installation des correctifs

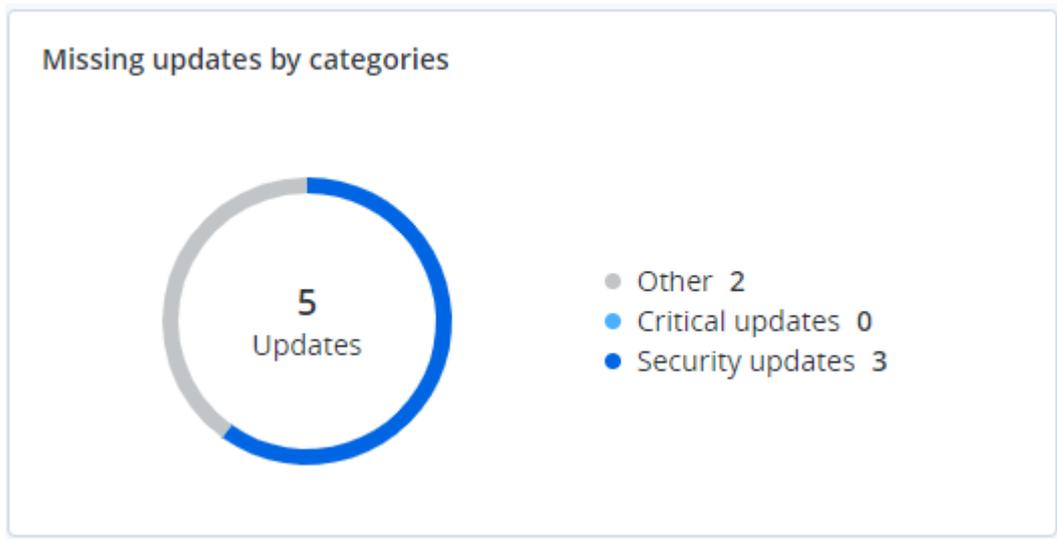
Ce widget affiche des informations détaillées au sujet des correctifs sur les machines.

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

Mises à jour manquantes, par catégorie

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

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



Détails de l'analyse de la sauvegarde

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

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen-Heur.PonyStealer.Im0@c05:cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen-Heur.PonyStealer.Im0@c05:cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen-Heur.PonyStealer.Im0@c05:cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen-Heur.PonyStealer.Im0@c05:cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen-Heur.PonyStealer.Im0@c05:cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

Affectés récemment

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

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlylgen2	15	27.12.2	Folder
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacrolg1	274	27.12.2	Customer
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2	✓ Machine name
Win2012_r2-Hyper-V	Protection plan	W97M.Downloaderlg32	5	27.12.2	✓ Protection plan
HyperV_for12A	Total protection	Miner.XMRigIgen1	68	27.12.2	Detected by
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2	✓ Threat
vm-sql_2012	Protection plan	Adware.DealPlylgen2	9	27.12.2	File name
MF_2012_R2	Total protection	MSH.DownloaderIgen8	73	27.12.2	File path
MF_2012_R2	Total protection	Bloodhound.MalMacrolg1	182	27.12.2	✓ Affected files
MF_2012_R2	Protection plan	Bloodhound.MalMacrolg1	18	27.12.2	✓ Detection time
ESXirestore	Protection plan	MSH.DownloaderIgen8	682	27.12.2017 11:23 AM	
MF_2012_R2	Protection plan	Miner.XMRigIgen1	13	27.12.2017 11:23 AM	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlylgen2	3	27.12.2017 11:23 AM	
Win2012_r2-Hyper-V	Total protection	W97M.Downloaderlg32	27	27.12.2017 11:23 AM	

[More](#) | [Show all 556](#)

Téléchargement de données pour les ressources récemment affectées

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

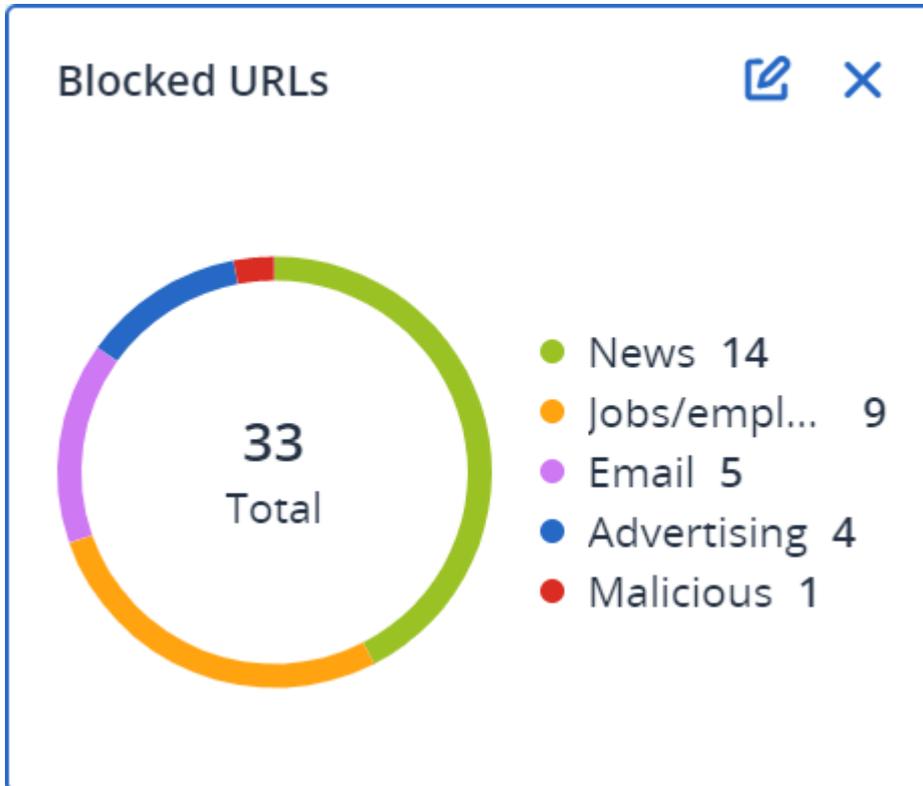
Pour télécharger les données pour les ressources récemment affectées

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

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

URL bloquées

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

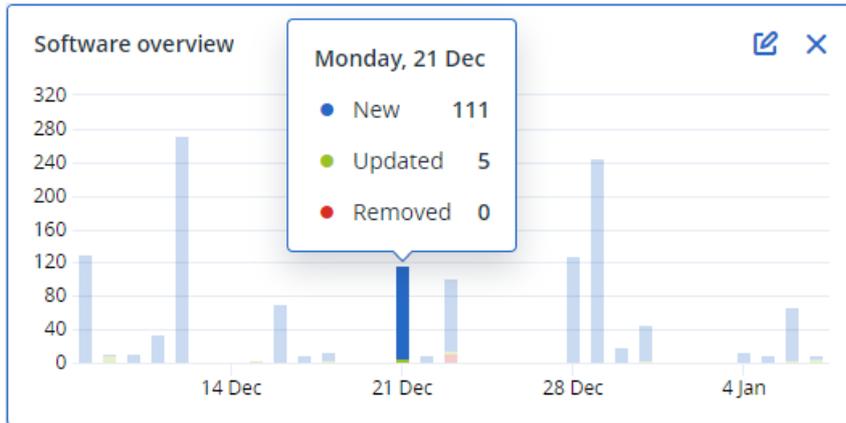


Widget d'inventaire du logiciel

Le widget de tableau **Inventaire du logiciel** contient des informations détaillées concernant tout le logiciel installé sur les terminaux physiques Windows et macOS de votre organisation.

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
~ 00003079									
00003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
00003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

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



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

Nouvelles – le nombre d'applications nouvellement installées.

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

Supprimées – le nombre d'applications supprimées.

Lorsque vous cliquez sur la partie de la barre correspondant à un certain statut, vous êtes redirigé vers la page **Gestion de logiciel** -> **Inventaire du logiciel**. Les informations de cette page sont filtrées en fonction de la date et du statut correspondants.

Widgets d'inventaire du matériel

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

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-mini-2.local	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
00003079.corp...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	NICET81W(11-49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local	CPU	To Be Filled By O.E.M.	Core i5, 3000, 6	Intel(R) Core(TM) i5-8500B CPU @ 3.00GHz	OK	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	RAM	4ATF51264HZ-2G6E3	9876543210, 4294...	1FACDD62	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	RAM	4ATF51264HZ-2G6E3	9876543210, 4294...	1FB057DA	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM

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

Hardware changes						
Machine name	Hardware category	Status	Old value	New value	Modification date and time	
▼ DESKTOP-0FF9TTF						
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3, ...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM	
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Toronto 5C1, PF0PJ810	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00.0...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM	

[More](#)

Historique des sessions

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

Remote sessions							
Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. 1.1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. 1.1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. 1.4
12/15/2022 1:...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1:...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

[More](#)

Widget de suivi de la géolocalisation

Sur le widget **Suivi de la géolocalisation**, vous pouvez voir des détails sur l'emplacement des ressources de votre organisation, tels que le pays, la ville ou la commune, les coordonnées, la dernière heure de détection et la méthode de suivi de la géolocalisation.

Geolocation tracking						1 day
Workload name	Method	Details	Country	City/Town	Last seen	
Long	OS	Lat. -34.5810, Long. -...	Argentina	Ciudad Autónoma de ...	02/11/2025 3:01 PM	
Chucks-Laptop	OS	Lat. 42.6826, Long. 2...	Bulgaria	Sofia City	02/11/2025 3:06 PM	

Widget de sessions de chat

Dans le widget **Sessions de chat**, vous pouvez afficher les détails des sessions de chat à distance dans votre organisation pour une période spécifiée.

Chat sessions									30 days
Start time	End time	Waiting time	Active time	Hold time	Total time	Technician name	Technician login	Workload ...	↑ ⚙
Mar 11, 2025 2:55 PM	Mar 11, 2025 3:11 PM	-	00:15:58	-	00:15:58	D Z	dz-con	WIN-PMJ2B9...	
Mar 4, 2025 12:31 PM	Mar 11, 2025 10:09 AM	21:12:24	21:38:13	00:00:04	00:25:53	Igor	igor	WIN-PMJ2B9...	
Mar 11, 2025 2:54 PM	Mar 11, 2025 2:55 PM	-	00:01:10	-	00:01:10	Borya	boryana	WIN-PMJ2B9...	
Mar 11, 2025 3:11 PM	Mar 11, 2025 6:24 PM	02:57:58	03:12:59	-	00:15:01	D Z	dz-con	WIN-PMJ2B9...	
Mar 11, 2025 6:24 PM	Mar 11, 2025 7:10 PM	00:30:31	00:46:00	-	00:15:28	D Z	dz-con	WIN-PMJ2B9...	
Feb 28, 2025 7:22 PM	Mar 3, 2025 5:16 PM	00:00:19	21:53:46	-	21:53:27	Igor	igor	WIN-PMJ2B9...	

Widget de performance du technicien

Dans le widget **Performance du technicien**, vous pouvez consulter les détails des performances de chaque technicien de votre organisation pour une période donnée.

Technician performance						30 days
Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration	↑ ⚙
Igor	igor	2	19:32:04	10:36:21	21:46:02	

Journal d'audit

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

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

- Opérations effectuées par les utilisateurs dans le portail de gestion
- Opérations avec des ressources de cloud à cloud effectuées par des utilisateurs dans la console Cyber Protect
- Opérations de création de cyberscripts effectuées par des utilisateurs dans la console Cyber Protect
- Opérations relatives à l'archivage des e-mails
- Messages système concernant les quotas atteints et l'utilisation des quotas

Le journal affiche les événements de l'organisation ou de l'unité dans laquelle vous fonctionnez actuellement, et de ses unités enfant. Vous pouvez cliquer sur un événement pour afficher davantage d'informations le concernant.

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

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

Champs de journal d'audit

Pour chaque événement, le journal affiche :

- **Événement**

Courte description de l'événement. Par exemple, **Tenant créé, Tenant supprimé, Utilisateur créé, Utilisateur supprimé, Le quota est atteint, Le contenu de la sauvegarde a été parcouru, Le script a été modifié.**

- **Gravité**

Peut être l'une des options suivantes :

- **Erreur**

Indique une erreur.

- **Avertissement**

Indique une action négative potentielle. Par exemple, **Tenant supprimé, Utilisateur supprimé, Le quota est atteint.**

- **Mentions légales**

Indique un événement qui peut nécessiter votre attention. Par exemple, **Tenant a été mis à jour, Utilisateur mis à jour.**

- **Informations**

Indique un changement ou une action informatifs neutres. Par exemple, **Tenant créé, Utilisateur créé, Le quota a été mis à jour, Le plan de création de script a été supprimé.**

- **Date**

Date et heure auxquelles l'événement a eu lieu.

- **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.

- **Tenant**

Nom de l'unité à laquelle l'objet appartient. Par exemple, le tenant de l'événement **Utilisateur mis à jour** est l'unité dans laquelle l'utilisateur est situé. Le tenant de l'événement **Le quota est atteint** est l'utilisateur dont le quota a été atteint.

- **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**.

- **Initiateur du tenant**

Nom de l'unité à laquelle l'initiateur appartient. Pour les messages système et les événements initiés par des administrateurs de haut niveau, le champ est vide.

- **Méthode**

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

- **IP**

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

Filtrer et rechercher

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

Collecte de données de performances pour les agents Cyber Protection

Pour les machines Windows protégées dans votre environnement, vous pouvez collecter les journaux de performances manuellement ou activer la collecte automatique des données de diagnostic si les performances du système tombent en dessous des seuils définis par défaut. Voir "Configuration des seuils de performances pour la collecte de données ETL" (p. 81).

Les journaux collectés sont anonymisés avant d'être envoyés pour analyse au fournisseur. Les données suivantes seront supprimées de tous les journaux, messages, alertes et messages d'erreur :

- Compte utilisateur
- Nom société
- Nom de la ressource protégée

En tant qu'administrateur de l'entreprise, vous pouvez activer la collecte automatique des journaux pour des agents sélectionnés aléatoirement ou pour des agents spécifiques dans votre organisation.

Remarque

- La collecte de données automatisée sur les ressources individuelles est prise en charge sur l'agent pour Windows Cyber Protection version 24.4.37758 ou ultérieure.
 - La collecte de données de performances au niveau du tenant est prise en charge sur l'agent pour Windows Cyber Protection version 25.03.XXXXX ou ultérieure.
-

Pour garantir que nos recommandations de support sont bien informées, nous recueillons des données provenant d'environ 10 % des agents de l'environnement pour analyse.

Cela ne remplace pas les paramètres des ressources individuelles. Par exemple, si la collecte de données automatisée est désactivée sur une ressource spécifique, cette ressource ne sera pas incluse dans la collecte de données en masse.

Collecte automatisée pour plusieurs agents

Pour activer la collecte automatisée des données de performances pour plusieurs agents dans un tenant

Rôle requis : Administrateur client

1. Dans la console Cyber Protect Cloud, accédez à **Paramètres > Agents**.
2. Dans le menu **Actions** à droite, cliquez sur **Modifier les paramètres du moniteur de performances**.
3. Dans la section **Moniteur de performances**, activez le bouton **Collecte et transfert automatiques des journaux de performances**.

Les données collectées automatiquement sont stockées sur les disques locaux des machines protégées, dans le dossier C:\ProgramData\Acronis\ETLTool\ETL\, anonymisées et envoyées au fournisseur de services pour analyse.

Remarque

La limite d'envoi des journaux ETL vers le cloud est de 3 fois en 24 heures.

Mises à jour automatiques d'un seul agent

Pour activer la collecte automatisée des données de performances pour un agent spécifique

1. Au niveau de l'entreprise dans la console Cyber Protect Cloud, accédez à **Paramètres > Agents**.
2. Dans la liste **Agents**, sélectionnez l'agent pour lequel vous souhaitez activer le moniteur de performances.
3. Dans le menu **Actions** à droite, cliquez sur **Détails**.
4. Faites défiler vers le bas jusqu'à la section **Moniteur de performances**, puis activez l'interrupteur **Autoriser cet agent à collecter automatiquement les journaux de performances**.

Les données collectées automatiquement sont stockées sur le disque local de la machine protégée dans le dossier C:\ProgramData\Acronis\ETLTool\ETL\.

Collecte manuelle

Pour collecter manuellement des données de performances

Vous pouvez collecter des données de performances à la demande, sans avoir à activer le moniteur de performances ni la collecte automatisée des données de performances.

1. Connectez-vous à l'ordinateur protégé en tant qu'administrateur.
2. À l'invite de commande, exécutez l'une des commandes suivantes :
 - "C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o
La collecte des traces ETL s'exécutera jusqu'à ce que vous appuyiez sur la touche S du clavier ou lorsque le délai maximal de 3 600 secondes sera écoulé.
 - "C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X
X est la limite de temps en secondes pour la collecte de données et la valeur maximale est 3 600. Vous pouvez arrêter la collecte à tout moment en appuyant sur la touche S du clavier.

Les données collectées manuellement sont stockées sur le disque local de l'ordinateur protégé, dans le dossier C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\

Pour collecter les journaux de performances

1. Connectez-vous à l'ordinateur protégé en tant qu'administrateur.
2. Recherchez les données dont vous avez besoin :
 - Les données de performances collectées automatiquement se trouvent dans le dossier
C:\ProgramData\Acronis\ETLTool\ETL\
 - Les données de performances collectées à la demande se trouvent dans le dossier
C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\

Les traces ETL sont également incluses dans le package sysinfo.

Configuration des seuils de performances pour la collecte de données ETL

Vous pouvez activer la collecte automatique des données de performance pour les machines Windows protégées de votre environnement. La surveillance est configurée par agent dans la console Cyber Protect Cloud et permet la collecte automatique de données de diagnostic si les performances du système chutent en dessous des seuils prédéfinis.

La collecte de données automatisée commence lorsqu'un des seuils est dépassé.

Seuils par défaut pour la collecte de données ETL

Le tableau suivant décrit les seuils qui déclenchent la collecte automatisée des données ETL.

Paramètre	Description	Valeur par défaut
"process-memory-consumption"	Seuil de surutilisation de la mémoire	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	Seuil d'utilisation élevée d'E/S du disque	
"maximum-operations-number"		10000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	Seuil d'utilisation élevée d'E/S de fichiers	

Paramètre	Description	Valeur par défaut
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	Seuil de consommation élevée du processeur	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	Performances des composants de l'agent de protection	
"behavioral-engine"	Seuil du moteur de comportement	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	Seuil du composant de protection antivirus et antimalware	
"average-scan-duration-seconds"	Durée maximale d'analyse moyenne	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	Durée maximale d'analyse unique	5

Rapports

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

Remarque

Cette fonctionnalité n'est pas disponible dans les éditions Standard du service Cyber Protection.

Rapports d'utilisation

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

Important

Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

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.

- **Résumé pour cette période**

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

Remarque

Les données d'utilisation du stockage local sont signalées uniquement au niveau de l'unité et du tenant client. Les utilisateurs ne reçoivent pas d'informations sur l'utilisation du stockage local dans les rapports récapitulatifs.

- **Jour par jour pour cette période**

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

Champ d'application du rapport

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

- **Clients directs et partenaires**

Le rapport comprendra uniquement les mesures d'utilisation de service pour les unités enfants immédiates de la société ou de l'unité dans laquelle vous travaillez.

- **Tous les clients et partenaires**

Le rapport comprendra les mesures d'utilisation de service pour les unités enfants de la société ou de l'unité dans laquelle vous travaillez.

- **Tous les clients et partenaires (y compris les informations d'utilisateur)**

Le rapport comprendra les valeurs des paramètres de rapport pour tous les tenants enfants du tenant dans lequel vous travaillez et pour tous les utilisateurs au sein des tenants.

Indicateurs avec zéro utilisation

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

Configuration de rapports d'utilisation planifiés

Un rapport planifié regroupe les mesures d'utilisation du service pour le mois précédent complet. Les rapports sont générés à 23:59:59 (UTC) le premier jour du mois et sont envoyés le second jour de ce même mois. Ils sont envoyés à tous les administrateurs de votre entreprise ou de votre unité 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 la société ou l'unité la plus haute disponible.
3. Cliquez sur **Rapports > Utilisation**.
4. Cliquez sur **Planifié**.
5. Cochez ou décochez la case **Envoyer un rapport de synthèse mensuel**.
6. Dans **Niveau de détail**, sélectionnez le champ d'application du rapport.
7. [Facultatif] Sélectionnez **Masquer les indicateurs avec zéro utilisation** si vous souhaitez exclure du rapport les indicateurs avec zéro utilisation.

Configuration de rapports d'utilisation personnalisés

Un rapport personnalisé est 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 l'unité](#) pour laquelle vous souhaitez créer un rapport.
3. Cliquez sur **Rapports > Utilisation**.
4. Cliquez sur **Personnalisé**.
5. Dans **Type**, sélectionnez le type de rapport.

6. [Non disponible pour le type de rapport **d'utilisation actuelle**] Dans **Période**, sélectionnez la période couverte par le rapport :
 - **Mois actuel**
 - **Mois précédent**
 - **Personnalisé**
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.
9. [Facultatif] Sélectionnez **Masquer les indicateurs avec zéro utilisation** si vous souhaitez exclure du rapport les indicateurs avec zéro utilisation.
10. Pour générer le rapport, cliquez sur **Générer et envoyer**.

Données des rapports d'utilisation

Le rapport sur l'utilisation du service Cyber Protection comprend les informations suivantes à propos d'une entreprise ou d'une unité :

- Le volume des sauvegardes par unité, par utilisateur et par type de terminal.
- Le nombre de terminaux protégés par unité, par utilisateur et par type de terminal.
- Prix par unité, utilisateur et type de terminal.
- Taille totale des sauvegardes.
- Nombre total de terminaux protégés.
- Prix total.

Si le service Cyber Protection ne parvient pas à détecter un type de terminal, ce terminal apparaît comme **Sans type** dans le rapport.

Important

Dans l'interface utilisateur de la solution, les valeurs d'utilisation du stockage sont affichées en octets binaires : mébioctets (Mio), gibioctets (Gio) et tébioctets (Tio). En revanche, les étiquettes affichent ces mêmes valeurs avec les unités Mo, Go et To. Par exemple, si l'utilisation réelle est de 3 105 886 629 888 octets, l'interface utilisateur affiche la valeur correcte de 2,82, mais avec l'unité To au lieu de l'unité Tio.

Rapports d'opération

Les rapports **Opérations** ne sont disponibles que pour les administrateurs d'entreprise lorsqu'ils travaillent à l'échelle de l'entreprise.

Un rapport au sujet des opérations peut inclure n'importe quel ensemble de widgets du [tableau de bord Opérations](#). Tous les widgets présentent le résumé pour l'ensemble de l'entreprise.

En fonction du type de widget, le rapport inclut les données pour une période ou pour le moment de la navigation ou de la génération de rapport. Consultez "Données rapportées en fonction du type de widget" (p. 103).

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

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

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

Les rapports par défaut sont répertoriés ci-dessous :

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

Activités hebdomadaires	Affiche des informations résumées au sujet des activités réalisées lors d'une période donnée.
Inventaire du logiciel	Affiche des informations détaillées concernant tout le logiciel installé sur les ordinateurs Windows et macOS de votre organisation.
Inventaire du matériel	Affiche des informations détaillées concernant tout le matériel disponible sur les ordinateurs physiques et virtuels Windows et macOS de votre organisation.
Sessions distantes	Affiche les informations détaillées concernant les sessions Bureau à distance et transfert de fichiers effectuées dans votre organisation pendant une période spécifiée.

Actions relatives aux rapports

Ajouter

Pour ajouter un nouveau rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Au bas de la liste des rapports disponibles, cliquez sur **Ajouter un rapport**.
3. [Pour ajouter un rapport prédéfini] Cliquez sur le nom du rapport prédéfini.
4. [Pour ajouter un rapport personnalisé] Cliquez sur **Personnalisé**, puis ajoutez des widgets au rapport.
5. [Facultatif] Glissez-déplacez les widgets pour les réorganiser.

Affichage

Pour afficher un rapport

- Pour afficher un rapport, cliquez sur son nom.

Modifier

Pour modifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez modifier.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Paramètres**.
4. Modifiez le rapport, puis cliquez sur **Enregistrer**.

Supprimer

Pour supprimer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez supprimer.

3. Dans l'angle supérieur droit de l'écran, cliquez sur l'icône représentant des points de suspension (...), puis sélectionnez **Supprimer le rapport**.
4. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

Planification

Pour planifier un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport que vous souhaitez planifier.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Paramètres**.
4. A côté de **Planifié**, activez le commutateur.
 - Spécifiez l'adresse e-mail des destinataires.
 - Sélectionnez le format du rapport.

- **Remarque**

Vous pouvez exporter jusqu'à 1 000 éléments dans un fichier PDF et jusqu'à 10 000 éléments dans un fichier XLSX. Les horodatages des fichiers PDF et XLSX utilisent l'heure locale de votre ordinateur.

- Sélectionnez la langue du rapport.
 - Configurez la planification.
5. Cliquez sur **Enregistrer**.

Télécharger

Pour télécharger un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Télécharger**.
4. Sélectionnez le format du rapport.

Un fichier du format sélectionné est téléchargé sur votre ordinateur.

Si vous avez sélectionné **Excel et PDF**, un fichier ZIP est téléchargé sur votre ordinateur.

Envoyer

Pour envoyer un rapport

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Dans le coin supérieur droit de l'écran, cliquez sur **Envoyer**.
4. Spécifiez l'adresse e-mail des destinataires.

5. Sélectionnez le format du rapport.
6. Cliquez sur **Envoyer**.

Exporter la structure

Pour exporter la structure des rapports

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport.
3. Dans le coin supérieur droit de l'écran, cliquez sur l'icône représentant des points de suspension (...), puis sur **Exporter**.

En conséquence, la structure du rapport est enregistrée sur votre ordinateur en tant que fichier JSON.

Vider les données

Pour vider les données du rapport

Vous pouvez exporter toutes les données d'une période personnalisée, sans les filtrer, vers un fichier CSV et envoyer ce fichier CSV à un destinataire par e-mail. Le fichier CSV ne contient que les données relatives aux widgets inclus dans le rapport.

Remarque

Vous pouvez exporter jusqu'à 150 000 éléments dans un fichier CSV. Les horodatages dans ce fichier CSV utilisent le temps universel coordonné (UTC).

1. Dans la console Cyber Protect, accédez à **Rapports**.
2. Dans la liste des rapports, sélectionnez le rapport dont vous souhaitez vider les données.
3. Dans le coin supérieur droit de l'écran, cliquez sur l'icône représentant des points de suspension (...), puis sur **Données de vidage**.
4. Spécifiez l'adresse e-mail des destinataires.
5. Dans la zone **Plage de temps**, spécifiez la période personnalisée pour laquelle vous souhaitez vider les données.

Remarque

La préparation des fichiers CSV pour de plus longues périodes prend plus de temps.

6. Cliquez sur **Envoyer**.

Synthèse

Le rapport de synthèse fournit une vue d'ensemble du statut de protection de l'environnement de votre organisation et des terminaux protégés pour une période spécifiée.

Le rapport de synthèse inclut des sections personnalisables avec des widgets dynamiques, qui affichent les indicateurs de performances clés liés à votre utilisation des services Cloud suivants : Sauvegarde, Protection antimalware, Évaluation de la vulnérabilité, Gestion des correctifs, Notary, Disaster Recovery et File Sync & Share.

Vous pouvez personnaliser le rapport de différentes manières.

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

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

Widgets de synthèse

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

Widgets d'aperçu des ressources

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

Widget	Description
Statut de protection des ressources Cloud	<p>Ce widget indique le nombre de ressources cloud protégées et non protégées par type au moment de la génération du rapport. Une ressource Cloud est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une ressource Cloud est considérée comme non protégée si aucun plan de protection ou de sauvegarde ne lui est appliqué. Les types de ressources Cloud suivants sont référencés dans le graphique (dans l'ordre alphabétique, de A à Z) :</p> <ul style="list-style-type: none"> • Drive Google Workspace • Gmail Google Workspace • Drive partagé Google Workspace • Boîtes aux lettres Exchange hébergées • Boîtes aux lettres Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams

Widget	Description
	<ul style="list-style-type: none"> • Sites Web <p>Pour certains types de ressources, les groupes de ressources suivants sont utilisés :</p> <ul style="list-style-type: none"> • Microsoft 365 : Utilisateurs, Groupes, Dossiers publics, Équipes et Collections de sites • Google Workspace : Utilisateurs et Disques partagés • Exchange hébergé : Utilisateurs <p>Si l'un des groupes de ressource contient plus de 10 000 ressources, le widget n'affiche pas de données correspondant à ces ressources.</p> <p>Par exemple, si votre organisation possède un compte Microsoft 365 avec 10 000 boîtes aux lettres et le service OneDrive pour 500 utilisateurs, étant donné que le tout est comptabilisé dans le même groupe de ressources Utilisateurs, la somme de ces ressources est de 10 500, ce qui dépasse la limite de 10 000 pour un groupe de ressources. Le widget masquera donc les types de ressources correspondants : Boîtes aux lettres Microsoft 365 et OneDrive Microsoft 365.</p>
<p>Résumé Cyber Protection</p>	<p>Ce widget affiche les indicateurs de performance clés de la cyberprotection pour une période spécifiée.</p> <p>Données sauvegardées : taille totale des archives créées dans les stockages local et Cloud.</p> <p>Menaces atténuées : nombre total de malware bloqués sur l'ensemble des terminaux.</p> <p>URL malveillantes bloquées : nombre total d'URL bloquées sur l'ensemble des terminaux.</p> <p>Vulnérabilités corrigées : nombre total de vulnérabilités qui ont été corrigées par l'installation de correctifs logiciels sur l'ensemble des terminaux.</p> <p>Correctifs installés : nombre total de correctifs installés sur l'ensemble des terminaux.</p> <p>Serveurs protégés par la RAS : nombre total de serveurs protégés par Disaster Recovery.</p> <p>Utilisateurs File Sync & Share : nombre total des utilisateurs finaux et invités qui utilisent Cyber Files.</p> <p>Fichiers notarisés : nombre total de fichiers notarisés.</p> <p>Documents signés de façon électronique : nombre total de documents signés de façon électronique.</p> <p>Périphériques bloqués : nombre total de périphériques bloqués.</p>

Widget	Description
Statut réseau des ressources	Ce widget affiche le nombre de ressources isolées et le nombre de ressources connectées (état normal des ressources).
Statut de protection des ressources	<p>Ce widget indique le nombre de ressources protégées et non protégées par type au moment de la génération du rapport. Une ressource est considérée comme protégée si au moins un plan de protection ou de sauvegarde lui est appliqué. Une ressource est considérée comme non protégée si aucun plan de protection ou de sauvegarde ne lui est appliqué. Les ressources suivantes sont prises en compte :</p> <p>Serveurs : serveurs physiques et serveurs contrôleur de domaine.</p> <p>Postes de travail : postes de travail physiques.</p> <p>Machines virtuelles : machines virtuelles avec agent et sans agent.</p> <p>Serveurs d'hébergement Web : serveurs virtuels or physiques avec cPanel ou Plesk installé.</p> <p>Terminaux mobiles : terminaux mobiles physiques.</p> <p>Une ressource peut appartenir à plusieurs catégories. Par exemple, un serveur d'hébergement Web est compté dans deux catégories : Serveurs et Serveurs d'hébergement Web.</p>
Terminaux découverts	<p>Le widget affiche les informations suivantes sur les terminaux découverts dans les réseaux de votre organisation au cours d'une période spécifiée :</p> <p>Nom du terminal</p> <p>Type de terminal</p> <p>Système d'exploitation</p> <p>Fabricant</p> <p>Modèle</p> <p>Adresse IP</p> <p>Adresse MAC</p> <p>Unité d'organisation</p> <p>Vous pouvez modifier le widget et filtrer les informations affichées par unité d'organisation, type de terminal, type de découverte, date de première découverte, date de dernière découverte, adresse IP, adresse MAC et type de découverte.</p>

Widgets de protection antimalware

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

Widget	Description
Analyse antimalware des fichiers	<p>Ce widget affiche les résultats des analyses antimalware effectuées à la demande sur les terminaux pour une période spécifiée.</p> <p>Fichiers : nombre total de fichiers analysés</p> <p>Propres : nombre total de fichiers propres</p> <p>Détectés, mis en quarantaine : nombre total de fichiers infectés mis en quarantaine</p> <p>Détectés, non mis en quarantaine : nombre total de fichiers infectés, non mis en quarantaine</p> <p>Terminaux protégés : nombre total de terminaux auxquels une règle de protection antimalware est appliquée</p> <p>Total de terminaux enregistrés : nombre total de terminaux enregistrés au moment de la génération du rapport</p>
Analyse antimalware des sauvegardes	<p>Ce widget affiche les résultats des analyses antimalware des sauvegardes pour une période spécifiée, en utilisant les indicateurs suivants :</p> <ul style="list-style-type: none"> • Nombre total de points de restauration analysés • Nombre de points de restauration propres • Nombre de points de restauration propres avec partitions non prises en charge • Nombre de points de restauration infectés. Cet indicateur inclut le nombre de points de restauration infectés avec partitions non prises en charge.
URL bloquées	<p>Ce widget affiche les URL bloquées classées par catégorie de site Web pour une période spécifiée.</p> <p>Le widget liste les sept catégories de site Web qui totalisent le plus grand nombre d'URL bloquées. Les autres catégories sont regroupées dans la section Autres.</p> <p>Pour plus d'informations sur les catégories de site Web, consultez la section dédiée au filtrage des URL dans Cyber Protection.</p>
Résolution des incidents de sécurité	<p>Ce widget indique l'efficacité de la clôture des incidents pour la société sélectionnée ; le nombre d'incidents ouverts est mesuré en fonction du nombre d'incidents clôturés pendant une période définie.</p> <p>Survolez une colonne pour afficher le détail des incidents clôturés et ouverts pour le jour sélectionné. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.</p>
MTTR de l'incident	<p>Ce widget affiche le temps de résolution moyen des incidents de sécurité. Il indique la vitesse à laquelle les incidents font l'objet d'enquêtes et sont résolus.</p> <p>Cliquez sur une colonne pour afficher le détail des incidents en fonction de la</p>

Widget	Description
	gravité (Critique, Élevé et Moyen), ainsi qu'une indication de la durée qui a été nécessaire à la résolution des différents niveaux de gravité. La valeur % figurant entre parenthèses indique l'augmentation ou la diminution par rapport à la période précédente.
Statut de la menace	Ce widget affiche le statut de menace actuel pour les ressources d'une entreprise (quel que soit le nombre de ressources) en mettant en évidence le nombre actuel d'incidents qui ne sont pas résolus et doivent faire l'objet d'enquêtes. Le widget indique également le nombre d'incidents résolus (manuellement et/ou automatiquement par le système).
Menaces détectées par la technologie de protection	Ce widget affiche le nombre de menaces détectées durant une période spécifique, classées selon les technologies de protection suivantes : <ul style="list-style-type: none"> • Analyse antimalware • Moteur de comportement • Protection contre le cryptomining • Prévention des failles • Protection active contre les ransomwares • Protection en temps réel • Filtrage d'URL

Widgets de sauvegarde

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

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

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

Widgets Évaluation des vulnérabilités et gestion des correctifs

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

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

Widgets de logiciels

Le tableau suivant fournit plus d'informations sur les widgets de la section **Logiciel**.

Widget	Description
Statut d'installation	Ce widget affiche le nombre total d'activités d'installation, regroupées par statut. En cliquant sur un segment du graphique en anneau, vous êtes redirigé vers la page Activités , où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.
État de la désinstallation	Ce widget affiche le nombre total d'activités de désinstallation, regroupées par statut. En cliquant sur un segment du graphique en anneau, vous êtes redirigé vers la page Activités , où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.
Historique d'installation des logiciels	Ce widget fournit des informations détaillées sur le statut des installations à distance de logiciels sur vos terminaux gérés. En cliquant sur un statut dans la colonne Statut d'installation , vous êtes redirigé vers la page Activités , où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.
Historique de désinstallation des logiciels	Ce widget fournit des informations détaillées sur le statut des désinstallations à distance de logiciels de vos terminaux gérés. En cliquant sur un statut dans la colonne Statut de désinstallation , vous êtes redirigé vers la page Activités , où seules les activités dont le statut correspond sont affichées, classées dans l'ordre chronologique.

Widgets de Disaster Recovery

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

Widget	Description
Statistiques de Disaster Recovery	<p>Ce widget affiche les indicateurs de performance clés du plan de Disaster Recovery pour la période spécifiée.</p> <p>Basculements de production : nombre d'opérations de basculement de production pour la période spécifiée.</p> <p>Basculements de test : nombre d'opérations de basculement test effectuées durant la période spécifiée.</p> <p>Serveurs primaires : nombre total de serveurs primaires existant au moment de la génération du rapport.</p> <p>Serveurs de restauration : nombre total de serveurs de restauration existant au moment de la génération du rapport.</p> <p>IP publiques : nombre total d'adresses IP publiques (existant au moment de</p>

Widget	Description
	<p>la génération du rapport).</p> <p>Total des points de calcul consommés : nombre total des points de calcul consommés durant la période spécifiée.</p>
<p>Serveurs de Disaster Recovery testés</p>	<p>Ce widget fournit des informations sur les serveurs protégés par Disaster Recovery et vérifiés avec le basculement test.</p> <p>Le widget affiche les indicateurs suivants :</p> <p>Serveurs protégés : nombre de serveurs protégés par Disaster Recovery (serveurs avec au moins un serveur de restauration) au moment de la génération du rapport.</p> <p>Testés : nombre de serveurs protégés par Disaster Recovery qui ont été vérifiés avec le basculement test au cours de la période spécifiée, par rapport au nombre total de serveurs protégés par Disaster Recovery.</p> <p>Non testés : nombre de serveurs protégés par Disaster Recovery qui n'ont pas été vérifiés avec le basculement test au cours de la période spécifiée, par rapport au nombre total de serveurs protégés par Disaster Recovery.</p> <p>Le widget indique également le volume en Go du stockage de Disaster Recovery au moment de la génération du rapport. Cela correspond à la somme des volumes de sauvegardes des serveurs Cloud.</p>
<p>Serveurs protégés par Disaster Recovery</p>	<p>Ce widget fournit des informations sur les serveurs protégés par Disaster Recovery et les serveurs non protégés.</p> <p>Le widget affiche les indicateurs suivants :</p> <p>Le nombre total de serveurs enregistrés dans le tenant client au moment de la génération du rapport.</p> <p>Protégés : nombre de serveurs protégés par Disaster Recovery (avec au moins un serveur de restauration et une sauvegarde de serveur complète), par rapport au nombre total de serveurs enregistrés au moment de la génération du rapport.</p> <p>Non protégés : nombre total de serveurs non protégés, par rapport au le nombre total de serveurs enregistrés au moment de la génération du rapport.</p>

Widget de prévention des pertes de données

Vous trouverez de plus amples informations sur les périphériques bloqués dans la section **Prévention des pertes de données** de la rubrique suivante.

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

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

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

Widget File Sync & Share

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

Widget	Description
Statistiques File Sync & Share	<p>Le widget affiche les indicateurs suivants :</p> <p>Total de stockage dans le Cloud utilisé : le total de stockage Cloud utilisé par tous les utilisateurs.</p> <p>Utilisateurs finaux : le nombre total d'utilisateurs finaux.</p> <p>Moyenne du stockage utilisé par utilisateur final : le stockage utilisé en moyenne par un utilisateur final.</p> <p>Utilisateurs invités : le nombre total d'utilisateurs invités.</p>
Utilisation du stockage File Sync & Share par les utilisateurs finaux	<p>Ce widget indique le nombre total d'utilisateurs File Sync & Share qui utilisent un stockage correspond aux plages suivantes :</p> <ul style="list-style-type: none"> • 0 à 1 Go • 1 à 5 Go • 5 à 10 Go • 10 à 50 Go • 50 à 100 Go • 100 à 500 Go • 500 Go à 1 To

Widget	Description
	<ul style="list-style-type: none"> Plus d'1 To

Widgets de Notary

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

Widget	Description
Statistiques Cyber Notary	<p>Le widget affiche les indicateurs Notary suivants :</p> <p>Stockage Notary Cloud utilisé : la taille totale du stockage utilisé pour le service Notary.</p> <p>Fichiers notariés : nombre total de fichiers notariés.</p> <p>Documents signés de façon électronique : le nombre total de documents et fichiers signés de façon électronique.</p>
Fichiers notariés pour l'ensemble des utilisateurs finaux	<p>Indique le nombre total de fichiers notariés pour l'ensemble des utilisateurs finaux. Les utilisateurs sont regroupés en fonction de leur nombre de fichiers notariés.</p> <ul style="list-style-type: none"> Jusqu'à 10 fichiers 11 à 100 fichiers 101 à 500 fichiers 501 à 1000 fichiers Plus de 1 000 fichiers
Documents signés de façon électronique pour l'ensemble des utilisateurs finaux	<p>Ce widget indique le nombre total de documents et fichiers signés de façon électronique pour l'ensemble des utilisateurs finaux. Les utilisateurs sont regroupés en fonction de leur nombre de fichiers et documents signés de façon électronique.</p> <ul style="list-style-type: none"> Jusqu'à 10 fichiers 11 à 100 fichiers 101 à 500 fichiers 501 à 1000 fichiers Plus de 1 000 fichiers

Configuration des paramètres du rapport de synthèse

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

Pour modifier les paramètres du rapport de synthèse

1. Dans la console de gestion, accédez à **Rapports>Synthèse**.
2. Cliquez sur le nom du rapport de synthèse dont vous souhaitez modifier les paramètres.
3. Cliquez sur **Paramètres**.

4. Modifiez les valeurs des champs selon vos besoins.
5. Cliquez sur **Enregistrer**.

Création d'un rapport de synthèse

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

Pour créer un rapport de synthèse

1. Dans la console de gestion, accédez à **Rapports>Synthèse**.
2. Cliquez sur **Créer un rapport de synthèse**.
3. Sous **Nom du rapport**, saisissez le nom du rapport.
4. Sélectionnez les destinataires du rapport.
 - Si vous souhaitez envoyer le rapport à tous les contacts et utilisateurs, sélectionnez **Envoyer à tous les contacts et utilisateurs**.
 - Si vous souhaitez envoyer le rapport à des contacts et utilisateurs spécifiques
 - a. Désélectionnez **Envoyer à tous les contacts et utilisateurs**.
 - b. Cliquez sur **Sélectionner des contacts**.
 - c. Sélectionnez les contacts et utilisateurs souhaités. Vous pouvez effectuer une Recherche pour trouver facilement un contact spécifique.
 - d. Cliquez sur **Sélectionner**.
5. Sélectionnez une plage : **30 jours** ou **Ce mois-ci**
6. Sélectionnez un format de fichier : **PDF**, **Excel** ou **Excel et PDF**.
7. Configurer les paramètres de planification.
 - Si vous souhaitez envoyer le rapport aux destinataires à une heure et une date spécifiques :
 - a. Activez l'option **Planifié**.
 - b. Cliquez sur le champ **Jour du mois**, désélectionnez Dernier jour, et cliquez sur le jour souhaité.
 - c. Dans le champ **Heure**, saisissez l'heure souhaitée.
 - d. Cliquez sur **Appliquer**.
 - Si vous souhaitez créer le rapport sans l'envoyer à ses destinataires, désactivez l'option **Planifié**.
8. Cliquez sur **Enregistrer**.

Personnalisation du rapport de synthèse

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

Pour ajouter une section

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

Pour renommer une section

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

Pour supprimer une section

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

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

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

Pour ajouter un widget personnalisé à une section

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

Pour ajouter un widget avec ses paramètres par défaut au rapport

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

Pour ajouter un widget personnalisé au rapport

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

Pour rétablir les paramètres par défaut d'un widget

1. Dans le widget que vous désirez personnaliser, cliquez sur **Modifier**.
2. Cliquez sur **Réinitialiser au défaut**.
3. Cliquez sur **Terminé**.

Pour personnaliser un widget

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

Envoi des rapports de synthèse

Vous pouvez envoyer un rapport de synthèse à la demande. Dans ce cas, le paramètre **Planifié** est ignoré, et le rapport est envoyé immédiatement. Pour l'envoi, le système utilise les valeurs de Destinataires, Plage et Format de fichier paramétrées dans les **Paramètres**. Vous pouvez modifier manuellement ces paramètres avant l'envoi du rapport. Pour plus d'informations, voir "Configuration des paramètres du rapport de synthèse" (p. 99).

Pour envoyer un rapport de synthèse

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

Le rapport envoie alors le rapport de synthèse aux destinataires sélectionnés.

Fuseaux horaires dans les rapports

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

Emplacement et type du rapport	Fuseaux horaires utilisés dans le rapport
Portail de gestion > Surveillance > 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 > Surveillance >	<ul style="list-style-type: none"> • L'horodatage du rapport exporté est indiqué dans le fuseau

Opérations (exporté vers PDF ou xlsx)	<p>horaire de la machine utilisée pour exporter le rapport.</p> <ul style="list-style-type: none"> Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Rapports > Utilisation > Rapports planifiés	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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 xlsx)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> Le fuseau horaire de la livraison du rapport est indiqué en UTC. Le fuseau horaire des activités affichées dans le rapport est indiqué en UTC.
Portail de gestion > Utilisateurs > Résumé quotidien concernant les alertes actives	<ul style="list-style-type: none"> Ce rapport est envoyé une fois entre 10:00 et 23:59 UTC. L'heure à laquelle le rapport est envoyé dépend de la ressource 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	<ul style="list-style-type: none"> Ce rapport est envoyé lorsqu'une activité est terminée. <hr/> <p>Remarque En fonction de la ressource du centre de données, il se peut que certains rapports soient envoyés en retard.</p> <hr/> <ul style="list-style-type: none"> Le fuseau horaire de l'activité du rapport est indiqué en UTC.

Données rapportées en fonction du type de widget

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

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

Lorsque vous configurez une plage de dates dans les paramètres de rapport afin d'effectuer un vidage mémoire des données d'une certaine période, la plage de dates sélectionnée s'applique

uniquement aux widgets qui affichent des données historiques. Elle n'est pas applicable aux widgets qui affichent les données actuelles au moment de la navigation ou de la génération du rapport.

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

Nom du widget	Données affichées dans le widget et les rapports
Score #CyberFit par machine	Actuelles
5 dernières alertes	Actuelles
Détails des alertes actives	Actuelles
Résumé des alertes actives	Actuelles
Activités	Historiques
Liste des activités	Historiques
Historique des alertes	Historiques
Analyse antimalware des sauvegardes	Historiques
Analyse antimalware des fichiers	Historiques
Détails de l'analyse de la sauvegarde (menaces)	Historiques
État de la sauvegarde	Historiques, dans les colonnes Total des exécutions et Nombre d'exécutions réussies Actuelles, dans toutes les autres colonnes
Utilisation du stockage de sauvegarde	Historiques
Périphériques bloqués	Historiques
URL bloquées	Actuelles
Applications dans le Cloud	Actuelles
Statut de protection des ressources Cloud	Actuelles
Cyberprotection	Actuelles
Résumé Cyber Protection	Historiques
Carte de la protection des données	Historiques
Terminaux	Actuelles
Serveurs de reprise d'activité après sinistre testés	Historiques
Statistiques de reprise d'activité après sinistre	Historiques

Terminaux découverts	Actuelles
Vue d'ensemble de l'état de santé du disque	Actuelles
Intégrité du disque	Actuelles
Intégrité de disque par terminaux physiques	Actuelles
Documents signés de façon électronique pour l'ensemble des utilisateurs finaux	Actuelles
Vulnérabilités existantes	Historiques
Statistiques File Sync & Share	Actuelles
Utilisation du stockage File Sync & Share par les utilisateurs finaux	Actuelles
Modifications apportées au matériel	Historiques
Détails du matériel	Actuelles
Inventaire matériel	Actuelles
Résumé de l'historique des alertes	Historiques
Résumé des emplacements	Actuelles
Mises à jour manquantes, par catégorie	Actuelles
Non protégé	Actuelles
Fichiers notarisés pour l'ensemble des utilisateurs finaux	Actuelles
Statistiques Notary	Actuelles
Historique d'installation des correctifs	Historiques
Statut d'installation des correctifs	Historiques
Résumé d'installation des correctifs	Historiques
Vulnérabilités corrigées	Historiques
Correctifs installés	Historiques
État de protection	Actuelles
Affectés récemment	Historiques
Sessions distantes	Historiques
Résolution des incidents de sécurité	Historiques
Temps moyen de réparation des incidents de	Historiques

sécurité	
Serveurs protégés par la reprise d'activité après sinistre	Actuelles
Inventaire du logiciel	Actuelles
Aperçu du logiciel	Historiques
Statut de la menace	Actuelles
Menaces détectées par la technologie de protection	Historiques
Distribution des principaux incidents par ressource	Actuelles
Machines vulnérables	Actuelles
Statut réseau des ressources	Actuelles
Ressources sauvegardées	Historiques
Statut de protection des ressources	Actuelles

Intégrations

Ce chapitre fournit les informations nécessaires pour trouver et activer des intégrations.

Les intégrations offrent des fonctionnalités de protection contre les cybermenaces tierces, de gestion des terminaux, de gestion des clients, de surveillance, d'analyse, etc., en parallèle des produits de la console Cyber Protect standard. Elles proposent également nos solutions via des plates-formes logicielles tierces. Plus de 200 intégrations automatisent actuellement les tâches quotidiennes et augmentent l'efficacité de nos partenaires et de leurs clients.

Les intégrations sont répertoriées dans les [catalogues d'intégrations](#).

Remarque

Certaines intégrations nécessitent un [client d'API](#) pour accéder aux interfaces de programmation d'application (API).

Catalogues des intégrations

Les catalogues des intégrations répertorient les intégrations disponibles :

- [Catalogue des applications](#).

Ce catalogue est accessible au public. Les intégrations ne peuvent pas être activées à partir de ce catalogue.

Si vous voyez une intégration que vous souhaitez utiliser, contactez votre partenaire pour qu'il l'active pour vous.

- [Catalogues de centres de données](#).

Ces catalogues sont propres au centre de données. Les intégrations peuvent être activées à partir de ces catalogues.

Les administrateurs du portail de gestion de niveau partenaire peuvent effectuer les opérations suivantes :

- Afficher toutes les intégrations déployées sur le centre de données.
- Activer toutes les intégrations déployées sur le centre de données, pour eux-même ou pour leurs clients.

Les administrateurs du portail de gestion au niveau du client peuvent effectuer les opérations suivantes :

- N'afficher que les intégrations définies explicitement par le développeur d'intégration comme étant visibles pour les clients.
- N'activer que les intégrations autorisées explicitement par le développeur d'intégration comme pouvant être activées par les clients.

Remarque

L'administrateur du portail de gestion au niveau du partenaire doit activer l'intégration au niveau du partenaire pour pouvoir être activé par un administrateur du portail de gestion au niveau du client.

Entrées du catalogue

Les entrées du catalogue sont constituées de deux parties :

- La fiche de catalogue fournit un aperçu de l'intégration.
- [La page de détails du catalogue](#) fournit d'autres informations : description fonctionnelle complète, captures d'écran, vidéos, liste de fonctionnalités, coordonnées, liens vers des ressources d'intégration, etc.

Ouverture de votre catalogue des intégrations du centre de données

Dans les catalogues d'intégration de centre de données (DC), survolez une carte de catalogue pour lire une brève description de la solution, le bouton **Configurer** et un lien **En savoir plus** :

- Le lien **En savoir plus**
Chaque entrée du catalogue des intégrations possède également une page comportant des détails sur l'intégration : description fonctionnelle complète, captures d'écran, vidéos, liste de fonctionnalités, coordonnées, liens vers des ressources d'intégration, etc.
Cliquez sur ce bouton pour ouvrir la page de détails de l'intégration.
- Le bouton **Configurer**
Cliquez sur ce bouton pour activer l'intégration.

Remarque

Les fiches de catalogue représentant des intégrations inactives apparaissent en grisé et sont désactivées.

Pour ouvrir votre catalogue des intégrations du centre de données

1. [Ouvrez le portail de gestion.](#)
2. Sélectionnez **Intégrations** dans le menu principal.
L'onglet **Toutes les intégrations** est ouvert par défaut. Il affiche les fiches de catalogue des intégrations que les administrateurs du portail de gestion de niveau client peuvent activer.
3. [Facultatif] Choisissez une catégorie et saisissez du texte dans le champ de recherche pour filtrer les cartes du catalogue.

Ouverture d'une page de détails d'intégration

Pour ouvrir une page de détails d'intégration

1. [Ouvrez le catalogue des intégrations dans votre centre de données.](#)
2. Localisez la carte de catalogue pour l'intégration.
3. Survolez la carte du catalogue.
4. Cliquez sur **En savoir plus**.

La page de détails de l'intégration s'ouvre.

Affichage de vos intégrations activées

L'onglet **Intégrations utilisées** du catalogue des intégrations affiche une fiche pour chaque intégration que vous avez activée.

Pour afficher vos intégrations activées

1. Ouvrez le [catalogue des intégrations](#) dans votre centre de données.
2. Sélectionnez l'onglet **Intégrations utilisées**.

Ouverture du catalogue d'applications

Le catalogue d'applications répertorie toutes les intégrations Cyber Protect Cloud.

Remarque

Si vous identifiez une intégration que vous souhaitez utiliser, vous devez contacter votre partenaire pour qu'il l'active pour vous.

Pour ouvrir le catalogue d'applications

1. Rendez-vous sur solutions.acronis.com.
La vue initiale répertorie dans une grille toutes les cartes de catalogue.
2. [Facultatif] Choisissez une catégorie et saisissez du texte dans le champ de recherche pour filtrer les cartes du catalogue.

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud
FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

All categories acronis

Security >

Data Protection >

Management >

Automation >

CloudBlue

Acronis Cyber Cloud Connect for Resellers

Ingram Micro

Acronis Cyber Protect Cloud for resellers provides full subscription live-cycle management.

Learn more

CloudBlue

Acronis Cyber Cloud Connect for End Customers

Acronis

Acronis Cyber Protect Cloud for end-customers provides full subscription live-cycle management.

Learn more

Acronis

Acronis Generic SIEM Connector

Acronis

Simplify security posture by integrating with SIEM platforms.

Learn more

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build Integration

Nominate a tool

Ouverture d'une page de détails d'intégration

Chaque entrée de catalogue dispose également d'une page avec des détails sur l'intégration : description fonctionnelle complète, captures d'écran, vidéos, liste de fonctionnalités, coordonnées, liens vers des ressources d'intégration, etc.

Pour ouvrir une page de détails d'intégration

1. Rendez-vous sur solutions.acronis.com.
2. Recherchez la fiche de catalogue de l'intégration qui vous intéresse.

3. Cliquez sur **En savoir plus** sur la fiche de catalogue.

Application Catalog

Integrations with the tools and services you know and trust

Contact us

Try Acronis



← Back to Integrations

Have a question or need help?

Acronis

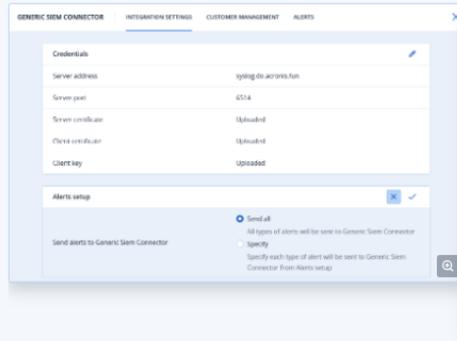
Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Website

Acronis Generic SIEM Connector

SIEM (Security Information and Event Management) platforms are used by many MSPs for security incident investigation and remediation, threat hunting, and compliance. Acronis Generic SIEM Connector allows MSPs to forward Acronis Cyber Protect Cloud alerts to any SIEM system that supports the CEF event format over SYSLOG for further correlation and analysis to reveal patterns of activity that may indicate an attempt of intrusion.

[Integration Overview](#)



Simplify security posture by integrating with SIEM platforms.

SIEMs empower MSPs security specialists to identify attack rout across the network and get visibility into compromised files. Now with Acronis Generic SIEM connector, MSPs will gain extra visibility into customers networks, will be able to search for threats across all managed workloads, and correlate events from both security and data protection applications, and run response actions.



Features

Support of core event format

Acronis supports core event format - CEF (Common Event Format), enabling MSPs to work with any SIEM that supports CEF format out of the box. Alerts are transferred to SIEM via syslog server.

Threat hunting across all managed companies

Integration allows MSPs to select which customer tenants in Acronis should send alerts to SIEM. Since alerts are sent to the same SIEM instance, it's possible to run correlation, threat hunting and perform investigation for all customers in the same console. It also empowers MSPs to search for threats, that were discovered on one workload in one customer tenant, in other customers environments.

Simple integration enablement

It's very easy to enable the integration by obtaining server and client certificates, establishing connection to the server and specifying the server port.

Select data you want to see

It is possible to select which alerts should be sent to SIEM. With this functionality, MSPs benefit from reducing the amount of sent to SIEM data and, therefore, lower SIEM invoice. MSPs can select and work only with the data that is necessary.

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build integration

Nominate a tool



Engage with Acronis



Activation d'une intégration

Remarque

L'administrateur du portail de gestion au niveau du partenaire doit activer l'intégration au niveau du partenaire pour pouvoir être activé par un administrateur du portail de gestion au niveau du client.

Pour activer une intégration

1. [Ouvrez le catalogue des intégrations dans votre centre de données.](#)
2. Recherchez la fiche de catalogue de l'intégration que vous souhaitez configurer.
Pour filtrer les intégrations :
 - [Facultatif] Sélectionnez une catégorie.
 - [Facultatif] Saisissez une chaîne dans le champ de recherche.
3. Survolez la carte du catalogue.
4. Cliquez sur **Configurer**.
5. Suivez les instructions affichées à l'écran.

Configuration d'une intégration active

Pour configurer une intégration active

1. [Ouvrez le catalogue des intégrations dans votre centre de données.](#)
2. Sélectionnez l'onglet **Intégrations utilisées**.
3. Recherchez la fiche de catalogue de l'intégration que vous souhaitez configurer.
4. Cliquez sur **Gérer**.
L'écran de configuration de l'intégration s'ouvre.
5. Suivez les instructions à l'écran ou consultez la documentation d'intégration.

Remarque

La documentation est généralement disponible dans la page de détails du catalogue. Pour plus d'informations, voir [Ouverture d'une page de détails d'intégration](#).

Désactivation d'une intégration active

Pour désactiver une intégration

1. [Ouvrez le catalogue des intégrations dans votre centre de données.](#)
2. Sélectionnez l'onglet **Intégrations utilisées**.
3. Recherchez la fiche de catalogue de l'intégration que vous souhaitez désactiver.

4. Cliquez sur **Désactiver**.
5. Cliquez sur **Supprimer**.

Clients de l'API

Les intégrations de systèmes tiers peuvent utiliser les 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.

Un client d'API est un compte de plate-forme spécial représentant le système tiers qui doit s'authentifier et être autorisé à accéder aux données de la plate-forme et des services. L'accès du client d'API est limité au tenant dont l'administrateur du portail de gestion crée le client, et à tous les sous-tenants.

Remarque

Le client d'API 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.

Identifiants du client d'API

Les identifiants du client d'API sont constitués de l'identifiant unique (ID) et d'une valeur secrète. Ils n'expirent pas et ne peuvent pas être utilisés pour établir la connexion au portail de gestion ni à aucune autre console de service.

Remarque

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

Flux du client d'API

1. Un administrateur du portail de gestion crée un client d'API.
2. Un administrateur active [le flux d'identifiants du client OAuth 2.0](#) dans le système tiers.
3. En fonction de ce flux, avant d'accéder au tenant et à ses services via l'API, le système doit d'abord envoyer les identifiants du client d'API à la plate-forme à l'aide de l'API d'autorisation.
4. La plate-forme génère et renvoie un jeton de sécurité, c'est-à-dire la chaîne chiffrée unique attribuée à ce client en particulier.
5. Le système tiers doit ajouter ce jeton à toutes les demandes d'API.

Remarque

Le jeton de sécurité évite d'avoir à passer par des demandes d'API pour obtenir les identifiants du client.

Pour une sécurité supplémentaire, le jeton de sécurité expire au bout de deux heures.

Passé ce délai, toutes les requêtes d'API avec le jeton expiré échouent et le système doit demander un nouveau jeton à la plate-forme.

Création d'un client d'API

Pour créer 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 le statut par défaut **Activé**.
5. Copiez et enregistrez l'ID et le code secret du client d'API, ainsi que l'URL du centre de données. Vous en aurez besoin pour activer le [flux d'identifiant du client OAuth 2.0](#) dans le 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. Toutefois, elle peut être réinitialisée.

6. Cliquez sur **Terminé**.

Réinitialisation de la valeur secrète d'un client d'API

Si vous perdez la valeur secrète du client d'API, vous pouvez en générer une nouvelle. L'identifiant du client et l'URL du centre de données ne changent pas.

Important

Si vous réinitialisez la valeur secrète, tous les jetons de sécurité affectés au client expirent immédiatement et les requêtes d'API avec ces jetons échouent.

Pour réinitialiser une valeur secrète de 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. Cliquez sur **Suivant** pour confirmer votre choix.
6. Copiez et enregistrez la nouvelle valeur secrète du client d'API.

Remarque

Pour des raisons de sécurité, la valeur secrète ne s'affiche qu'une seule fois. Il n'existe aucun moyen de récupérer cette valeur si vous la perdez. Pour la réinitialiser, vous devrez répéter ces étapes.

7. Cliquez sur **Terminé**.

Désactiver un client d'API

Vous pouvez désactiver les clients d'API. Dans ce cas, les requêtes d'API avec des jetons de sécurité qui sont affectés au client échoueront, mais les jetons n'expireront pas immédiatement.

Remarque

Désactiver le client n'affecte pas le délai d'expiration des jetons.

Vous pouvez [réactiver le client d'API](#) à tout moment.

Pour 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.

Activation d'un client d'API désactivé

Si vous activez un client d'API précédemment désactivé, les requêtes d'API avec des jetons de sécurité qui sont affectés au client aboutiront **si ces jetons n'ont pas encore expiré**.

Pour activer 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**.

Le statut du un client d'API passe à **Activé**.

Suppression d'un client d'API

Si vous supprimez un client d'API, tous les jetons de sécurité qui lui sont affectés expireront immédiatement et les requêtes d'API avec ces jetons échoueront.

Important

Il est impossible de restaurer un client supprimé.

Pour supprimer 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.

Création d'une intégration

Si vous avez des données ou des services que vous souhaitez intégrer à Cyber Protect Cloud, vous pouvez créer une CyberApp native à l'aide du portail des fournisseurs ou utiliser des appels d'API.

CyberApp

Le portail dédié aux fournisseurs est une plate-forme en ligne qui permet aux éditeurs de logiciels tiers d'intégrer des solutions et des services de manière native dans Cyber Protect Cloud, conformément à nos bonnes pratiques CyberApp Standard. Les intégrations dans le portail dédié aux fournisseurs sont appelées CyberApps.

Remarque

Pour plus d'informations sur les CyberApps et le portail des fournisseurs, consultez le [Guide d'intégration](#).

Intégrations des API

Il existe une suite complète d'API pour les intégrations.

Remarque

Pour plus d'informations sur les API, consultez [le chapitre sur les API de la plate-forme du Guide d'intégration](#).

Index

A

- À propos de ce document 6
- À propos du portail de gestion 7
- Accès au portail de gestion et aux services 21
- Activation d'un client d'API désactivé 116
- Activation d'un compte administrateur 20
- Activation d'une intégration 113
- Activation de la formation avancée de sensibilisation à la sécurité pour les utilisateurs de votre organisation 50
- Affectés récemment 73
- Affichage de l'utilisation du stockage immuable 49
- Affichage de vos intégrations activées 109
- Affichage des tickets auprès du service d'assistance 53
- Afficher les quotas pour votre organisation 10
- Alertes relatives à l'état de santé du disque 68

C

- Carte de la protection des données 68
- Catalogues des intégrations 107
- Champ d'application du rapport 83
- Champs de journal d'audit 77
- Clients de l'API 114
- Collecte de données de performances pour les agents Cyber Protection 79
- Comptes et unités 8
- Configuration d'un stockage immuable 47
- Configuration d'une intégration active 113

- Configuration de l'authentification à deux facteurs pour vos tenants 38
- Configuration de rapports d'utilisation personnalisés 84
- Configuration de rapports d'utilisation planifiés 84
- Configuration des mises à jour de l'agent Cyber Protection 42
- Configuration des paramètres du rapport de synthèse 99
- Configuration des seuils de performances pour la collecte de données ETL 81
- Configurer l'authentification à deux facteurs 35
- Création d'un client d'API 115
- Création d'un compte utilisateur 22
- Création d'un rapport de synthèse 100
- Création d'un ticket auprès du service d'assistance 53
- Création d'une intégration 117
- Création d'une unité 22
- CyberApp 117

D

- Désactivation d'une intégration active 113
- Désactivation et activation d'un compte utilisateur 33
- Désactiver un client d'API 116
- Détails de l'analyse de la sauvegarde 72
- Distribution des principaux incidents par ressource 62
- Données des rapports d'utilisation 85
- Données rapportées en fonction du type de

widget 103

Intégrations des API 117

E

Empêcher les utilisateurs de Microsoft 365 sans licence de se connecter 15

Entrées du catalogue 108

Envoi des rapports de synthèse 102

État de protection 60

Exemple de facturation pour le stockage immuable 50

Exigences relatives au mot de passe 20

F

Filtrer et rechercher 79

Flux du client d'API 114

Fonctionnement 35, 65

Fuseaux horaires dans les rapports 102

G

Gestion de l'authentification à 2 facteurs pour les utilisateurs 39

Gestion des quotas 9

Gestion des tâches 53

H

Historique d'installation des correctifs 71

Historique des sessions 76

I

Identifiants du client d'API 114

Indicateurs avec zéro utilisation 84

Instructions pas-à-pas 20

Intégrations 107

J

Journal d'audit 77

L

La modification des paramètres de notification pour un utilisateur 29

Limitation de l'accès à l'interface Web 51

Limites 49, 64

Limitez l'accès à votre société 52

M

Ma boîte de réception 7

Machines vulnérables 69

Mise à jour des tickets auprès du service d'assistance 55

Mises à jour manquantes, par catégorie 72

Modes de stockage immuable 47

MTTR de l'incident 62

N

Navigateurs Web pris en charge 7

Navigation dans le portail de gestion 21

Notifications activées par défaut par type de terminal et rôle d'utilisateur 32

O

Ouverture d'une page de détails d'intégration 108, 110

Ouverture de votre catalogue des intégrations du centre de données 108

Ouverture du catalogue d'applications 109

P

- Paramètres de notification par défaut activés par type de notification et rôle de l'utilisateur 31
- Passer du portail de gestion aux consoles de service, et vice-versa 21
- Personnalisation du rapport de synthèse 101
- Pour activer l'authentification à deux facteurs pour un utilisateur 41
- Pour désactiver l'authentification à 2 facteurs 39
- Pour désactiver l'authentification à deux facteurs pour un utilisateur 40
- Pour réinitialiser l'authentification à deux facteurs pour un utilisateur 39
- Pour réinitialiser les navigateurs fiables pour un utilisateur 40
- Propagation de la configuration de l'authentification à deux facteurs à tous les niveaux de tenants 37
- Protection contre les attaques en force brute 41

Q

- Quota pour le stockage 18
- Quotas d'envoi de données physiques 17
- Quotas de Disaster Recovery 15
- Quotas de sauvegarde 10, 18
- Quotas pour la File Sync & Share 16, 19
- Quotas pour le stockage 14
- Quotas pour les sources de données Cloud 10
- Quotas pour Notary 17, 19
- Quotas principaux pour vos utilisateurs 17

R

- Rapports 83
- Rapports d'opération 85
- Rapports d'utilisation 83
- Recherche dans Ma boîte de réception 8
- Réinitialisation de l'authentification à deux facteurs en cas de perte du terminal qui applique le second facteur 41
- Réinitialisation de la valeur secrète d'un client d'API 115
- Résolution des incidents de sécurité 63
- Résumé d'installation des correctifs 71
- Rôle d'administrateur en lecture seule 27
- Rôle d'opérateur de restauration 28
- Rôles utilisateur disponibles pour chaque service 25

S

- Score #CyberFit par machine 61
- Seuils par défaut pour la collecte de données ETL 81
- Soumission de tickets de service d'assistance via le portail de tickets 56
- Statut d'installation des correctifs 71
- Statut réseau des ressources 63
- Stockage immuable 46
- Stockages et agents pris en charge 47
- Suppression d'un client d'API 116
- Suppression d'un compte utilisateur 33
- Surveillance 39, 58
- Surveillance de l'intégrité du disque 64
- Synthèse 89

T

Tableau de bord des opérations 59
Téléchargement de données pour les
ressources récemment affectées 73
Terminaux découverts 60
Transférer la propriété d'un compte
utilisateur 34
Type de rapport 83

U

URL bloquées 74
Utilisation 58

V

Vérification de vos notifications 8
Vue d'ensemble 7
Vulnérabilités existantes 70

W

Widget d'inventaire du logiciel 74
Widget de performance du technicien 77
Widget de prévention des pertes de
données 97
Widget de sessions de chat 76
Widget de suivi de la géolocalisation 76
Widget File Sync & Share 98
Widgets d'aperçu des ressources 90
Widgets d'évaluation des vulnérabilités 69
Widgets d'installation des correctifs 71
Widgets d'inventaire du matériel 75
Widgets de Disaster Recovery 96

Widgets de Endpoint Detection and Response
(EDR) 61

Widgets de l'état de santé du disque 65

Widgets de logiciels 96

Widgets de Notary 99

Widgets de protection antimalware 92

Widgets de sauvegarde 94

Widgets de synthèse 90

Widgets Évaluation des vulnérabilités et gestion
des correctifs 95