

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a white, rounded rectangular area that is set against a background of green and teal abstract shapes.

kaspersky

Kaspersky Managed Detection and Response

© 2026 AO Kaspersky Lab

Contenu

[Aide de Kaspersky Managed Detection and Response](#)

[Nouveautés](#)

[À propos de Kaspersky Managed Detection and Response](#)

[Principe de fonctionnement de Kaspersky Managed Detection and Response](#)

[Domaines de responsabilité](#)

[Configuration matérielle et logicielle requise](#)

[Modules de Kaspersky Managed Detection and Response](#)

[Activation et déploiement de Kaspersky Managed Detection and Response](#)

[Composants nécessaires au fonctionnement de la solution MDR](#)

[Intégration avec les applications et solutions Kaspersky](#)

[Configuration du plug-in MDR](#)

[Activation et déploiement de MDR en cas d'utilisation de versions à jour des applications et d'un locataire unique](#)

[Activation et déploiement de MDR en cas d'utilisation de versions à jour des applications et de la multilocation](#)

[Activation et déploiement de MDR en cas d'utilisation d'anciennes versions des applications](#)

[Déploiement d'un fichier de configuration KPSN](#)

[Déploiement d'un fichier de configuration MDR \(BLOB\)](#)

[Déploiement par capture et copie de l'image d'un appareil](#)

[Activation de la solution MDR dans les applications Kaspersky](#)

[Activation de la solution MDR dans les applications Kaspersky. Licences pour modules complémentaires Kaspersky MDR](#)

[Activation de la solution MDR dans les applications Kaspersky. Licences Kaspersky MDR](#)

[Activation de la solution MDR dans les applications Kaspersky. Licences Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security et Kaspersky Next MXDR Optimum](#)

[Activation de la solution MDR dans les applications Kaspersky. Licence pour le module complémentaire de Kaspersky Managed Detection and Response for Industrial CyberSecurity.](#)

[Licence](#)

[Comparatif des niveaux de licence commerciale](#)

[À propos du code d'activation](#)

[Entrez un nouveau code d'activation](#)

[Gestion des licences dans Kaspersky Security Center](#)

[Résolution des problèmes de licence](#)

[À propos de l'Accord MDR](#)

[Collecte des données](#)

[Régions de traitement des données](#)

[À propos de l'Accord sur le traitement des données](#)

[Interfaces de Kaspersky Managed Detection and Response](#)

[Section MDR dans Kaspersky Security Center](#)

[Configuration du plug-in MDR dans Kaspersky Security Center](#)

[Configuration des droits d'accès dans Kaspersky Security Center](#)

[Consultation et modification des paramètres MDR dans Kaspersky Security Center](#)

[Utilisation des fonctions du plug-in MDR sur un Serveur d'Administration virtuel](#)

[Utilisation des fonctions MDR de Kaspersky Security Center via un serveur proxy.](#)

[Modification des certificats pour l'utilisation des fonctions MDR dans Kaspersky Security Center grâce à un serveur proxy ou un logiciel antivirus](#)

[Masquer et afficher les fonctionnalités MDR dans Kaspersky Security Center](#)

[Console MDR en ligne](#)

[Changement de la langue de l'interface dans Kaspersky Security Center](#)

[Changement de langue pour les notifications et les rapports dans Kaspersky Security Center](#)

[Changement de langue de l'interface dans la Console MDR en ligne](#)

[À propos du fichier de configuration MDR](#)

[À propos de Kaspersky Security Network](#)

[Mise à jour périodique des fichiers de configuration KPSN](#)

[Basculement de la solution MDR vers un fonctionnement sans fichiers de configuration KPSN](#)

[Tableaux de bord de surveillance dans de la Console MDR en ligne](#)

[Réception d'informations récapitulatives](#)

[Recevoir un résumé de toutes les ressources sous forme de fichier CSV \(Console MDR en ligne\)](#)

[Réception des informations sur l'incident au format PDF \(Console MDR en ligne\)](#)

[Configuration de l'envoi régulier de rapports dans la Console MDR en ligne](#)

[Réception de notifications](#)

[Configuration des notifications dans la Console MDR en ligne](#)

[Notifications sur l'état des ressources](#)

[Réception de notifications détaillées](#)

[Activation des notifications détaillées dans la Console MDR en ligne](#)

[Administration des utilisateurs](#)

[Invitation de nouveaux utilisateurs dans la Console MDR en ligne](#)

[Modification des rôles des utilisateurs dans la Console MDR en ligne](#)

[Modification des modes de notification des utilisateurs dans la Console MDR en ligne](#)

[Modification de l'accès des utilisateurs aux clients dans la Console MDR en ligne](#)

[Suppression de comptes utilisateurs](#)

[Gestion des ressources](#)

[Affichage et recherche dans les ressources de la Console MDR en ligne](#)

[Filtrage des ressources dans la Console MDR en ligne](#)

[Affichage d'informations détaillées concernant les ressources dans la Console MDR en ligne](#)

[États des ressources](#)

[Vérification de l'état des ressources dans Kaspersky Security Center](#)

[Éviter la perte des données de télémétrie des ressources](#)

[Administration des incidents](#)

[À propos des incidents](#)

[Visualisation et recherche des incidents dans la Console MDR en ligne](#)

[Filtrage des incidents dans la Console MDR en ligne](#)

[Création d'incidents personnalisés dans la Console MDR en ligne](#)

[Affichage d'informations détaillées concernant les incidents dans la Console MDR en ligne](#)

[Traitement des réponses aux incidents dans la Console MDR en ligne](#)

[Types de réponse](#)

[Acceptation automatique des réponses dans la Console MDR en ligne](#)

[Acceptation automatique des réponses dans Kaspersky Security Center](#)

[Clôture des incidents dans la Console MDR en ligne](#)

[Envoi d'un incident à l'équipe de réponse aux incidents pour une enquête complémentaire](#)

[Intégration de Kaspersky Unified Monitoring and Analysis](#)

[Création d'incidents de Managed Detection and Response à partir d'incidents XDR](#)

[Intégration de Kaspersky Digital Footprint Intelligence pour MDR](#)

[Utilisation des fonctionnalités de Kaspersky Endpoint Detection and Response Expert](#)

[Réponses](#)

[Gestion des locataires](#)

[Gestion des locataires dans Kaspersky Security Center](#)

[Affichage des clients dans Kaspersky Security Center](#)

[Affichage des paramètres des locataires dans Kaspersky Security Center](#)

[Modification des paramètres des locataires dans Kaspersky Security Center](#)

[Ajout de nouveaux locataires dans Kaspersky Security Center](#)

[Suppression des locataires dans Kaspersky Security Center](#)

[Déplacement de ressources entre locataires](#)

[Gestion des locataires dans la Console MDR en ligne](#)

[Affichage des locataires dans la Console MDR en ligne](#)

[Affichage des paramètres des locataires dans la Console MDR en ligne](#)

[Modification des paramètres des locataires dans la Console MDR en ligne](#)

[Ajout de nouveaux locataires dans la Console MDR en ligne](#)

[Suppression des locataires dans la Console MDR en ligne](#)

[Gestion de la solution via l'API REST](#)

[Scénario : effectuer une autorisation basée sur des jetons](#)

[Création d'une connexion API dans Kaspersky Security Center](#)

[Création d'une connexion API dans la Console MDR en ligne](#)

[Modification d'une connexion API dans Kaspersky Security Center](#)

[Modification d'une connexion API dans la Console MDR en ligne](#)

[Création d'un jeton d'accès à Kaspersky Security Center](#)

[Création d'un jeton d'accès dans la Console MDR en ligne](#)

[Utilisation de l'API REST](#)

[Révocation du jeton d'actualisation dans Kaspersky Security Center](#)

[Suppression d'une connexion API dans Kaspersky Security Center](#)

[Suppression d'une connexion API dans la Console MDR en ligne](#)

[Désactivation de Kaspersky Managed Detection and Response](#)

[Arrêt de l'utilisation de Kaspersky Managed Detection and Response](#)

[Suspension de l'utilisation de Kaspersky Managed Detection and Response](#)

[Révocation de votre consentement avec les conditions d'utilisation de la solution MDR](#)

[Problèmes connus](#)

[Contacter le Support Technique](#)

[Modes d'obtention du support technique](#)

[Assistance technique via le Kaspersky CompanyAccount](#)

[Sources d'informations à propos de la solution](#)

[Glossaire](#)

[Application EPP](#)

[Incident](#)

[IOC](#)

[Locataire](#)

[Plateforme de protection des terminaux \(EPP\)](#)

[Réponse](#)

[Ressource](#)

[Tactique MITRE](#)

[Technique MITRE](#)

[Télémétrie](#)

[Informations sur le code tiers](#)

[Avis de marques commerciales](#)

Aide de Kaspersky Managed Detection and Response



Nouvelles fonctions

- [Nouveautés de la dernière version de la solution](#)



Configurations logicielle et matérielle

- [Vérifiez les systèmes d'exploitation et les applications EPP pris en charge](#)



Comparaison des fonctionnalités

- [Comparatif des solutions sous licence commerciale : MDR Optimum, MDR Expert, MDR Basic, MDR Advanced et MDR Prime](#)



Prise en main

- Déploiement sur site
- Déploiement basé sur le cloud
- [Activation de Kaspersky Managed Detection and Response](#)



Suivi et rapports

- [Réception de notifications](#)
- [Réception de notifications détaillées](#)
- [Réception d'informations récapitulatives](#)
- [Tableaux de bord de suivi](#)



Collecte de données / Protection des données personnelles

- [Collecte des données](#)
- [Kaspersky Security Network](#)

Nouveautés

Kaspersky Managed Detection and Response présente différentes nouvelles fonctionnalités et améliorations.

Août 2026

Le plug-in MDR version 3.11, destiné à Open Single Management Platform version 2.2, est désormais disponible.

Juillet 2026

- Notifications sur l'état des ressources

MDR prend désormais en charge [l'envoi automatique de notifications lorsque l'état de vos ressources protégées requiert votre attention](#). Configurez les valeurs de seuil pour les états de ressources OK, Warning, Critical et Offline, et recevez des notifications par email ou Telegram lorsque les conditions configurées sont remplies. Cela vous permet de détecter rapidement les problèmes de collecte de télémétrie ou de connectivité sans surveiller en permanence la page Assets.

Juin 2026

- Intégration de Kaspersky DFI pour MDR

Notre service MDR exploite désormais les renseignements sur les informations d'identification compromises du service Kaspersky DFI afin d'améliorer les flux de travail de détection, d'investigation et de recherche des menaces. En établissant un lien entre les identifiants divulgués et les événements de sécurité, puis en intégrant ces informations dans des activités proactives de recherche des menaces, MDR peut détecter plus tôt les compromissions potentielles de comptes, améliorer la hiérarchisation des incidents et contribuer à réduire le risque d'accès non autorisés.

Fonctionnalités clés :

- Enrichissement des alertes en tenant compte du contexte des identifiants divulgués
 - Corrélation entre les identifiants divulgués et les incidents de sécurité
 - Recherche des menaces et détection des compromissions basées sur les identifiants
 - Matrice de compatibilité des applications avec MDR mise à jour
- Le tableau Applications et solutions Kaspersky compatibles a été mis à jour. Certaines versions héritées de produits ont été déplacées dans la catégorie Compatibilité MDR limitée (certaines fonctionnalités MDR peuvent ne pas être disponibles), tandis que la prise en charge de Kaspersky Endpoint Agent a été interrompue. Pour en savoir plus, consultez [l'article mis à jour dans l'aide en ligne](#).

Mai 2026

- Le plug-in MDR version 3.0.2, destiné à Open Single Management Platform version 2.1, est désormais disponible.
- Les utilisateurs peuvent désormais laisser un commentaire directement lors de la clôture d'un incident dans la Console MDR. Cela permet d'améliorer la qualité du service et de mieux évaluer la satisfaction des clients.
- Les administrateurs MDR peuvent désormais [définir la limite de ressources attendue pour chaque locataire](#) dans la Console MDR.

Si le nombre de ressources connectées dépasse la limite configurée, une notification s'affichera à la fois dans la liste des locataires et sur la page des propriétés du locataire. Cela permet aux administrateurs de suivre de manière proactive l'étendue de l'intégration et les prévisions en matière de licences.

Cette fonctionnalité sera intégrée au plug-in MDR dans une prochaine version.

- Le format des notifications envoyées par email et via Telegram a été amélioré afin d'en faciliter la lecture et de permettre un accès plus rapide aux informations importantes.

Cette mise à jour concerne les notifications relatives aux :

- Incidents
- Remarques formulées lors des échanges avec les analystes MDR
- Actions de réponse
- Mises à jour de l'état de la clé de licence

Mars 2026

Ajout de la prise en charge de Kaspersky Embedded Systems Security for Linux version 4.0 ou ultérieure. Vous pouvez désormais [activer la solution MDR](#) dans Kaspersky Embedded Systems Security for Linux avec une licence Kaspersky MDR.

Décembre 2025

- Ajout de la prise en charge des applications EPP suivantes :
 - Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure
 - Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5
- Vous pouvez désormais configurer des [notifications Telegram étendues](#) dans le plug-in MDR en plus de la console MDR en ligne.
- Vous pouvez [envoyer des incidents à l'équipe de réponse aux incidents à des fins d'enquête supplémentaire](#) via l'interface de la console MDR en ligne.

- Ajout de la prise en charge des solutions Kaspersky suivantes :
 - Intégration à Kaspersky Endpoint Detection and Response version 8.0 ou ultérieure qui active les fonctionnalités suivantes :
 - [Possibilité de créer des incidents MDR à partir d'incidents XDR.](#)
 - [Type de réponse](#) Get artefacts.
 - Intégration à Kaspersky Anti Targeted Attack version 8.0 ou ultérieure, qui ajoute le Get artefacts [Obtenir les artefacts.](#)

Consultez l'article suivant : [Intégration aux applications et aux solutions Kaspersky](#)

Octobre 2025

Vous pouvez désormais configurer des [notifications Telegram détaillées](#) dans la Console MDR en ligne.

Juillet 2025

- Ajout de la possibilité d'utiliser des codes d'activation pour activer la solution MDR dans les applications suivantes :
 - Kaspersky Endpoint Security for Linux version 12.3
 - Kaspersky Endpoint Security for Linux version 12.3 en mode Light Agent
 - Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure
 - Kaspersky Endpoint Security for Windows version 12.8 ou ultérieure en mode Light Agent
 - Kaspersky Endpoint Security for Mac version 12.2

Pour en savoir plus, consultez l'article suivant : [Activation de la solution MDR dans les applications Kaspersky.](#)
- La solution MDR peut désormais fonctionner sans le fichier de configuration KPSN avec les applications suivantes :
 - Kaspersky Endpoint Security for Linux version 12.3
 - Kaspersky Endpoint Security for Linux version 12.3 en mode Light Agent
 - Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure
 - Kaspersky Endpoint Security for Windows version 12.8 ou ultérieure en mode Light Agent
 - Kaspersky Endpoint Security for Mac version 12.2

Pour en savoir plus, reportez-vous à l'article suivant : [Basculement de la solution MDR vers un fonctionnement sans fichiers de configuration KPSN.](#)

- La solution MDR prend désormais en charge [Kaspersky Endpoint Security for Windows version 12.8 ou ultérieure en mode Light Agent](#) ².
- La version 2.5.1 du plug-in MDR prend désormais en charge le fonctionnement MDR sans le fichier de configuration KPSN.
- Kaspersky Endpoint Security for Linux version 12.3 prend désormais en charge les actions de réponse suivantes :
 - Isoler
 - Désactiver l'isolement
 - Fichier de quarantaine
 - Restaurer le fichier depuis la quarantaine
 - Terminer le processus
 - Exécuter le processus

Mai 2025

- Dans la section [Licences](#) du plug-in MDR pour Kaspersky Security Center :
 - Pour chaque licence MDR, le nom du client auquel la licence est délivrée est désormais affiché.
 - La matrice d'utilisation des licences spécifiques dans les locataires est désormais disponible.
- Dans la section [Locataires](#) du plug-in MDR pour Kaspersky Security Center :
 - Lors de la création d'un fichier de configuration MDR pour une licence spécifique, le nom du client pour lequel la licence est émise est désormais affiché.
 - La liste des locataires affiche désormais le locataire racine, qui est créé par défaut après l'activation du client. Vous pouvez télécharger les fichiers de configuration pour toutes les licences actuelles du locataire racine.

Février 2025

- La Console MDR en ligne comporte désormais la section **Licensing**. On y retrouve les fonctionnalités suivantes :
 - Affichage des licences MDR en cours, inutilisées et expirées.
 - Affichage du nombre total de ressources et de leur limite pour chaque licence.

- Téléchargement du fichier de configuration MDR pour le locataire racine.

Utilisation de [la section Locataires](#) afin de créer et de télécharger des fichiers de configuration MDR pour d'autres locataires.

- Saisie d'un nouveau code d'activation.

Si votre organisation dispose de plusieurs licences, vous ne pouvez les gérer que dans le plug-in MDR pour Kaspersky Security Center. La section **Licensing** de la Console MDR en ligne passe en lecture seule.

- Le plug-in MDR pour Kaspersky Security Center prend désormais en charge [l'utilisation de plusieurs licences](#) dans votre organisation. On y retrouve les fonctionnalités suivantes :
 - Affichage des licences MDR en cours, inutilisées et expirées.
 - Résiliation d'une licence MDR actuelle.
 - Saisie d'un nouveau code d'activation.
 - Téléchargement du fichier de configuration MDR du locataire racine pour une licence.
 - Choix d'une licence pour un fichier de configuration MDR lors de la création ou de la modification d'un locataire dans [la section Locataires](#).

Décembre 2024

- Activation simplifiée de Kaspersky Managed Detection and Response sur les appareils Kaspersky Endpoint Security for Windows (à partir de la version 12.4). Tout ce dont vous avez besoin est une licence standard pour l'activation de la solution Kaspersky MDR.

Notez que vous devrez toujours utiliser le fichier de configuration MDR (BLOB) dans l'un des scénarios suivants :

- Vous avez plusieurs locataires.
- Vous utilisez la solution MDR conjointement avec Kaspersky Endpoint Detection and Response Optimum.
- Ajout de la prise en charge de la gestion de la solution MDR dans Kaspersky Security Center Linux (à partir de la version 15.1).
- Des [renseignements détaillés sur les exigences en matière de canaux de communication ont été ajoutés](#) dans l'aide.

Octobre 2024

Lancement du plug-in MDR pour Kaspersky Security Center version 2.4.1 Elle contient les améliorations suivantes :

- La possibilité de configurer l'acceptation automatique des actions d'intervention pour certains locataires a été ajoutée dans le plug-in MDR pour Kaspersky Security Center.
- Amélioration des fonctionnalités et de l'interface utilisateur de la [section indiquant la liste des ressources inactives](#). Ces ressources ont été ajoutées à Kaspersky Security Center, ont le module MDR installé, mais n'ont jamais transmis de données télémétriques à Kaspersky Managed Detection and Response. Vous pouvez filtrer les ressources selon leur état dans la solution MDR, consulter les informations détaillées de chaque ressource et exporter la liste des ressources dans un fichier au format CSV.

Cette fonctionnalité fonctionne correctement dans Kaspersky Security Center 15.1 Windows ou versions ultérieures, Kaspersky Security Center 15.1 Linux ou versions ultérieures, et Kaspersky Next Expert View.

- [La tâche de remise régulière d'un rapport sur les incidents ouverts](#) ne peut être créée que dans la Console MDR en ligne. Cette fonctionnalité a été supprimée de la section MDR de Kaspersky Security Center.

Juillet 2024

La Console MDR en ligne permet désormais de paramétrer l'acceptation automatique des actions d'intervention pour les locataires sélectionnés.

Juin 2024

- De nouvelles [actions de réponse](#) sont désormais disponibles :
 - Mettre le fichier en quarantaine
 - Restaurer le fichier depuis la quarantaine
 - Exécuter un script sur une ressource
- Mise à jour de [la documentation de l'API REST](#), notamment de nouveaux exemples de script.
- [Rapports](#) entièrement repensés :
 - Mappage MITRE ATT&CK pour une analyse approfondie des menaces.
 - Liste des ordinateurs les plus ciblés par les cybercriminels pour permettre aux clients de se concentrer sur les risques critiques.

- Prise en charge de plusieurs locataires :
 - Générez des rapports et [configurez un calendrier de rapports généraux](#) pour des locataires particuliers.
 - Basculez facilement des widgets aux statistiques d'un locataire dans le [tableau de bord de surveillance](#).
 - Configurez la confirmation automatique de l'exécution de la tâche de réponse pour des locataires particuliers.
 - API MDR améliorée pour la gestion des locataires.

Décembre 2023

- La Console MDR en ligne contient à présent le tableau de bord **Telemetry statistics**, qui affiche le nombre d'événements de télémétrie, d'événements de sécurité et d'incidents.
- Kaspersky Managed Detection and Response prend désormais en charge Kaspersky Endpoint Security for Windows dans la configuration de Endpoint Detection and Response Agent (EDR Agent) (avec les [restrictions](#)).

Novembre 2023

- Amélioration de l'affichage des états des ressources dans la Console MDR en ligne et dans le plug-in MDR pour Kaspersky Security Center : l'[état de la ressource](#) affiche désormais l'opérabilité des modules d'application EPP de la ressource, l'état de mise à jour de la base antivirus et l'état de la transmission des données télémétriques.
- L'état de la ressource affiche désormais la présence de pertes de données télémétriques de celle-ci, ce qui vous permet d'identifier les ressources présentant des problèmes d'envoi des données télémétriques. Cette fonctionnalité est activée par défaut pour les nouveaux clients et sera activée progressivement pour les clients existants.

Octobre 2023

La région de résidence du client **Arabie Saoudite** est ajoutée. Pour ces clients, les données télémétriques sont stockées au Royaume d'Arabie Saoudite.

Septembre 2023

Lancement du plug-in MDR pour Kaspersky Security Center version 2.3.1. Dans cette version, les fonctions de gestion des incidents de la section MDR de Kaspersky Security Center ont été supprimées. Vous pouvez également gérer les incidents dans la [Console MDR en ligne](#).

Juillet 2023

Lancement du plug-in MDR pour Kaspersky Security Center version 2.3.0. Elle contient les améliorations suivantes :

- Vous pouvez désormais configurer des notifications détaillées dans le plug-in MDR.
- Vous pouvez désormais utiliser les fonctions MDR dans Kaspersky Security Center doté du plug-in MDR au moyen d'un serveur proxy.
- Vous pouvez désormais modifier les certificats pour utiliser les fonctions MDR de Kaspersky Security Center avec un serveur proxy ou un logiciel antivirus.

Juillet 2022

Publication de la version 2.1.17 du plug-in MDR. Cette version du plug-in est compatible avec Kaspersky Security Center version 14 ou ultérieure.

Mai 2022

Améliorations générales :

- La région de résidence du client **États-Unis/Canada** a été ajoutée. Pour ces clients, leurs données de télémétrie sont stockées en Europe du Nord.
- Modification de la description du processus de déploiement de MDR dans l'aide.

Améliorations du plug-in MDR :

- Dans la section **Paramètres**, vous pouvez désormais modifier la langue des notifications envoyées dans Telegram et par e-mail ainsi que pour la communication dans le chat concernant les incidents.
- Interface améliorée pour travailler avec des images et des tableaux dans les cartes d'incidents.
- MDR Expert. Dans la section **Utilisation du service**, vous pouvez vérifier combien d'incidents peuvent être créés selon l'accord de niveau de service.

Corrections de bugs et autres améliorations :

- La recherche dans les listes d'incidents et de ressources est désormais effectuée par une occurrence complète de la sous-chaîne recherchée n'importe où dans la chaîne.
- Dans Kaspersky Endpoint Security for Mac version 11.2 ou ultérieure, après avoir saisi le code d'activation MDR et ajouté le fichier de configuration KPSN, vous n'avez plus besoin de redémarrer votre appareil Mac pour lancer un transfert de télémétrie.
- Lors du calcul des licences pour les machines virtuelles avec Kaspersky Security for Virtualization Light Agent version 5.2 ou ultérieure, les ressources qui n'ont pas transféré de télémétrie depuis plus de 24 heures ne sont pas prises en compte.

Mars 2022

Les utilisateurs de [MDR Optimum](#) peuvent désormais chatter avec les analystes de Kaspersky SOC au sujet d'un incident (avec la limitation suivante : les demandes ne sont traitées que pour un incident particulier et aucun accord de niveau de service n'est appliqué).

Octobre 2021

- Le plug-in Kaspersky Managed Detection and Response pour Kaspersky Security Center Web Console et Kaspersky Next Expert View a été mis à jour avec la [fonctionnalité améliorée États des ressources MDR](#) :
 - Amélioration de l'interface de l'onglet États des ressources MDR.
 - La liste des ressources affiche toutes les ressources de tous les états qui étaient auparavant disponibles uniquement dans la Console MDR en ligne.
 - Ajout d'options de filtrage et de tri pour la liste des ressources.

Juillet 2021

- Prise en charge de Kaspersky Managed Detection and Response dans Kaspersky Next Expert View, qui permet de gérer la solution dans la console d'administration unique de Kaspersky Security Center. Les fonctionnalités suivantes sont disponibles pour la solution Kaspersky Managed Detection and Response :
 - [Gestion des incidents](#) :
 - Visualiser, créer et commenter des incidents
 - Contacter Kaspersky Security Operation Center à propos d'un incident, accepter ou rejeter les réponses suggérées par les analystes SOC
 - [Répondre à un incident à l'aide de Kaspersky Endpoint Detection and Response](#)

Les fonctionnalités suivantes sont disponibles :

- Application de l'isolement du réseau des appareils
- Créer des règles de blocage par hash
- Créer des tâches de suppression, de mise en quarantaine, de fin de processus et de recherche par indicateurs de compromission (IOC), liés à un incident
- [Surveillance des événements de Kaspersky Managed Detection and Response sur les tableaux de bord](#) dans la console de surveillance de Kaspersky Security Center Web Console
- [Configuration des notifications](#) sur les événements de Kaspersky Managed Detection and Response par e-mail et via Telegram
- [Paramétrage du planning de résumé des performances du MDR](#) envoyé par e-mail
- [Affichage des appareils sur lesquels il y a des problèmes](#) de performances MDR
- [Nouvel assistant d'activation](#), qui permet de connecter MDR dans Kaspersky Security Center Web Console
- [Configuration automatique de KPSN](#), qui ne nécessite plus le téléchargement et le chargement manuels du fichier de configuration dans les paramètres de Kaspersky Security Center
- [Gestion des connexions à l'API publique MDR](#) : visualisation, création, modification et suppression des jetons
- [Gestion des locataires de l'organisation, y compris leur création](#)
- Obtenir des informations sur le nombre d'incidents disponibles pour l'enregistrement du côté de l'utilisateur, et qui sont éligibles pour le traitement selon les conditions du contrat de niveau de service (SLA)

Ces fonctionnalités sont également disponibles dans Kaspersky Security Center Web Console.

- La gestion de plusieurs comptes Administrateur MDR a été ajoutée dans la Console MDR en ligne : création des comptes et gestion des privilèges de compte

- Les nouvelles versions des applications compatibles ne nécessitent plus l'installation supplémentaire de Kaspersky Endpoint Agent. La fonctionnalité intégrée de Kaspersky Managed Detection and Response est compatible avec les applications EPP suivantes :

- Kaspersky Endpoint Security for Windows version – version 11.6 ou ultérieure
- Kaspersky Endpoint Security for Mac 11.2
- Kaspersky Endpoint Security for Linux 11.2
- Kaspersky Security for Virtualization 5.2 Light Agent

Pour plus de détails sur les différents scénarios de déploiement, consultez [Déploiement de Kaspersky Managed Detection and Response](#).

- Le filtrage par type d'événement a été ajouté pour Kaspersky Endpoint Security for Windows et Linux avec la fonctionnalité Kaspersky Managed Detection and Response intégrée, qui permet de réduire la charge sur les canaux et la consommation de trafic lors de l'envoi de données par télémétrie
- Prise en charge des types de réponse suivants : [obtenir un fichier à partir de l'appareil, désactiver l'isolement de l'appareil, supprimer la clé de registre](#), terminer le processus.

Ces actions sont possibles après confirmation de l'utilisateur disposant du rôle Administrateur MDR.

- Prise en charge des nouvelles localisations suivantes dans le plug-in Internet pour Kaspersky Security Center Web Console et Kaspersky Next Expert View : français, allemand, italien et espagnol.

Mars 2021

Un nouveau plug-in Web pour Kaspersky Security Center Web Console permet d'utiliser les fonctionnalités suivantes de Kaspersky Managed Detection and Response :

- Affichage d'incidents
- Création d'incidents
- Ajout de commentaires aux incidents
- Contact de Kaspersky Security Operation Center à propos d'un incident
- Acceptation ou refus des réponses suggérées par les analystes du SOC
- Possibilité de réponse indépendante à un incident :
 - Isoler des ressources du réseau
 - Créer des règles de blocage par hachage
 - Créer des tâches de suppression, de mise en quarantaine, de fin de processus et de recherche par indicateurs de compromission (IOC), liés à un incident
- Surveillance des événements de Kaspersky Managed Detection and Response sur les tableaux de bord dans la console de surveillance de Kaspersky Security Center Web Console

- Configuration des notifications par e-mail et par Telegram à propos des événements de Kaspersky Managed Detection and Response
- Paramétrage du planning de résumé des incidents envoyé par e-mail

À propos de Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response est une solution qui détecte et analyse automatiquement les incidents de sécurité dans votre infrastructure à l'aide de technologies de télémétrie et d'apprentissage automatique avancées, puis transfère les informations concernant l'incident aux experts de Kaspersky. Les experts peuvent alors soit traiter l'incident eux-mêmes, soit donner des recommandations sur la manière de le traiter.

Kaspersky Managed Detection and Response (également appelé MDR) offre une protection 24 heures sur 24 contre le volume croissant de menaces qui contournent les barrières de sécurité automatisées aux organisations qui ont des difficultés à trouver l'expertise et le personnel, ou à celles dont les ressources internes sont limitées. La solution permet d'améliorer la résilience de votre entreprise aux cybermenaces, tout en libérant vos ressources existantes pour que vous puissiez vous concentrer sur d'autres tâches.

Contrairement à des offres similaires sur le marché, cette solution s'appuie sur une expérience éprouvée de recherche efficace sur les attaques ciblées pour assurer une défense continue contre les menaces les plus complexes.

La solution Kaspersky Managed Detection and Response (MDR) n'est pas disponible aux États-Unis ni pour les ressortissants américains. L'utilisation de la solution MDR sur le territoire indiqué ou par des personnes résidant aux États-Unis constitue une violation des [conditions d'utilisation de la solution MDR](#). Pour éviter la violation des conditions d'utilisation de la solution MDR, il est nécessaire de [mettre fin définitivement à l'utilisation de la solution MDR](#) sur toutes les ressources situées dans le territoire indiqué ou par des personnes résidant aux États-Unis. Lorsque des personnes non américaines se trouvent temporairement aux États-Unis, elles sont tenues [suspendre l'utilisation de la solution MDR](#) sur leurs ressources.

Principe de fonctionnement de Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response analyse les données de télémétrie des applications EPP et génère des événements de sécurité qui peuvent être classés comme incidents par la technologie de détection.

Kaspersky Managed Detection and Response reçoit les données des applications EPP qui prennent en charge MDR, traite les données et les envoie via les flux [Kaspersky Security Network](#) à Kaspersky Managed Detection and Response. Pour la liste des données traitées, reportez-vous à la section [Collecte des données](#). Les applications EPP sont installées sur des ressources au sein de l'infrastructure informatique de votre organisation (par exemple, des ressources mobiles, des ordinateurs ou des ordinateurs portables). Kaspersky Endpoint Security for Windows est un exemple d'application EPP.

La Console MDR en ligne sert à traiter les incidents. Vous pouvez également intégrer Kaspersky Managed Detection and Response à une solution tierce, comme décrit dans l'article [Gestion de la solution via l'API REST](#).

La solution Kaspersky Managed Detection and Response peut résoudre un incident automatiquement ou demander une réponse de l'utilisateur à une menace pour la sécurité. Consultez l'article [Types de réponse](#) pour plus de détails. Pour garantir une réponse rapide aux éventuelles menaces pour la sécurité, la solution Kaspersky Managed Detection and Response peut vous demander des précisions concernant un événement suspect. Vous devez traiter ces demandes à temps.

L'enquête détaillée sur l'incident (comme l'établissement des événements précédents, des circonstances et du mécanisme détaillé de l'attaque mené par le pirate informatique) est gérée par le composant Kaspersky Incident Response. Il n'est pas inclus dans Kaspersky Managed Detection and Response et doit être acheté séparément.

L'utilisation de Kaspersky Managed Detection and Response implique que vous traitiez les incidents avec l'aide des experts de Kaspersky. Consultez l'article pour plus d'informations : [Domaines de responsabilité](#).

Domaines de responsabilité

L'utilisation de Kaspersky Managed Detection and Response implique que les utilisateurs traitent les incidents avec l'aide de la solution MDR. De plus, le Support technique de Kaspersky gère les problèmes liés à la solution.

Le tableau ci-dessous indique les domaines de responsabilité des utilisateurs, de la solution MDR et du Support technique de Kaspersky.

Tâche	La solution MDR	Support technique de Kaspersky	Utilisateurs MDR
Activation de MDR, déploiement de MDR, gestion des ressources, configuration des notifications, gestion des utilisateurs, résiliation de l'utilisation de MDR	–	Consultation	Effectuer la tâche
Utilisation de la Console MDR en ligne pour gérer les incidents	–	Consultation	Effectuer la tâche
Détection, enquête et émission de recommandations de réponse aux incidents en fonction des données télémétriques	Effectuer la tâche	–	Recevoir des informations
Clarification des détails lors de l'enquête, réponses aux questions de la solution MDR pour des recommandations de réponse améliorées	Recevoir des informations	–	Effectuer la tâche
Création de demandes d'utilisation des outils et des fonctionnalités de la solution MDR pour gérer les incidents.	Effectuer la tâche	–	Recevoir des informations
Coordination des demandes d'utilisation des outils et des fonctionnalités de la solution MDR pour gérer les incidents.	Recevoir des informations	–	Effectuer la tâche
Exécution de tâches en dehors des capacités fonctionnelles de MDR	Consultation	–	Effectuer la tâche
Création manuelle d'un incident (il est important de choisir une ressource MDR et de décrire l'incident en détail)	Recevoir des informations	–	Effectuer la tâche
Gestion des problèmes liés aux composants de l'infrastructure Kaspersky qui affectent la solution MDR	Recevoir des informations	Consultation	Effectuer la tâche
Gestion des règles de détection	Effectuer la tâche	–	–

Configuration matérielle et logicielle requise

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Applications EPP requises et configurations prises en charge

Pour pouvoir utiliser Kaspersky Managed Detection and Response, au moins une des applications EPP suivantes doit être déployée dans votre infrastructure :

- Ordinateurs portables, ordinateurs de bureau, tablettes et serveurs
 - [Kaspersky Endpoint Security for Windows](#) 
 - [Kaspersky Endpoint Security for Linux](#) 
 - [Kaspersky Endpoint Security for Mac](#) 
- Terminaux industriels
 - [Kaspersky Industrial CyberSecurity for Nodes Windows](#) 
- Systèmes virtuels
 - [Kaspersky Security for Virtualization Light Agent](#) 
- Systèmes embarqués
 - [Kaspersky Embedded Systems Security for Windows](#) 
 - [Kaspersky Embedded Systems Security for Linux](#) 
- Surveillance des événements réseau
 - [Kaspersky Anti Targeted Attack Platform](#) 

Systèmes d'exploitation

Kaspersky Managed Detection and Response est compatible avec les mêmes systèmes d'exploitation que les applications EPP répertoriées ci-dessous. Pour plus de détails, reportez-vous à la section *Configuration matérielle et logicielle requise* dans la documentation des applications EPP compatibles répertoriées dans le tableau ci-dessous.

Applications et solutions Kaspersky compatibles

Kaspersky Managed Detection and Response est compatible avec les versions des applications Kaspersky répertoriées dans le tableau ci-dessous.

Application Kaspersky	Versions recommandées et leur durée de prise en charge	Compatibilité MDR limitée *	Remarques
Kaspersky Endpoint Security for Windows	12.10 ou version ultérieure	12.6–12.9	Les versions 12.6 à 12.9 de Kaspersky Endpoint Security for Windows prennent en charge l'activation de la solution MDR à l'aide d'un code d'activation. La version 12.10 ou ultérieure de Kaspersky Endpoint Security for Windows prend en charge l'activation de la solution MDR à l'aide d'un fichier clé.
Kaspersky Endpoint Security for Windows en mode Light Agent	12.9 ou version ultérieure	12.8	Les versions 12.6 à 12.9 de Kaspersky Endpoint Security for Windows en mode Light Agent prennent en charge l'activation de la solution MDR à l'aide d'un code d'activation. Kaspersky Endpoint Security for Windows 12.10 ou ultérieure en mode Light Agent prend également en charge l'activation de la solution MDR à l'aide d'un fichier clé.
Kaspersky Endpoint Security for Windows dans la configuration de Endpoint Detection and Response Agent (EDR Agent) À compter de la version 12.3 de Kaspersky Endpoint Security for Windows, l'application inclut la configuration de Endpoint Detection and Response Agent (EDR Agent). Endpoint Detection and Response Agent est une application qui est installée sur les postes de travail et les serveurs dans l'infrastructure informatique de l'entreprise en soutien aux solutions Kaspersky Managed Detection and Response et Kaspersky Anti Targeted Attack Platform (EDR). EDR Agent surveille en continu les processus exécutés sur ces ordinateurs, les connexions réseau ouvertes et les fichiers en cours de modification. Les modules de protection et de contrôle ne sont pas disponibles pour EDR Agent. EDR Agent est compatible avec les applications EPP tierces. Cela vous permet d'utiliser des outils tiers de sécurité de l'infrastructure avec Detection and Response by Kaspersky. Pour en savoir plus, consultez l'aide en ligne de Kaspersky Endpoint Security for Windows.	12.8 ou version ultérieure	12.6–12.7	- En ce qui concerne les ressources associées à Kaspersky Endpoint Security for Windows dans la configuration de EDR Agent, les états <i>Avertissement</i> et <i>Critique</i> des composants de protection et de contrôle ne sont pas affichés. - Vous ne pouvez pas utiliser les fonctionnalités de Kaspersky Endpoint Detection and Response Optimum pour les ressources associées à Kaspersky Endpoint Security for Windows dans la configuration de EDR Agent. - La liste des applications EPP tierces compatibles avec EDR Agent est fournie dans l' aide en ligne de Kaspersky Endpoint Security for Windows. Les versions 12.6 à 12.9 de Kaspersky Endpoint Security for Windows dans la configuration de Endpoint Detection and Response Agent (EDR Agent) prennent en charge l'activation de la solution MDR à l'aide d'un code d'activation. Kaspersky Endpoint Security for Windows version 12.10 ou ultérieure dans la configuration de Endpoint Detection and Response Agent (EDR Agent) prend également en charge l'activation de la solution MDR à l'aide d'un fichier clé.

Application Kaspersky	Versions recommandées et leur durée de prise en charge	Compatibilité MDR limitée *	Remarques
Kaspersky Endpoint Security for Linux	12.4 ou version ultérieure 	12.1-12.3 	Si vous utilisez Kaspersky Endpoint Security for Linux et que vous n'avez pas installé le paquet Linux Audit Daemon (également appelés auditd), les événements d'audit système sont consignés dans le journal du noyau dmesg. Nous vous recommandons d'installer le paquet auditd pour faciliter la gestion de la rotation des journaux. La version 12.3 ou ultérieure de Kaspersky Endpoint Security for Linux prend en charge l'activation de la solution MDR à l'aide d'un fichier clé et d'un code d'activation.
Kaspersky Endpoint Security for Linux en mode Light Agent	12.4 ou version ultérieure 	12.1-12.3 	La version 12.3 ou ultérieure de Kaspersky Endpoint Security for Linux en mode Light Agent prend en charge l'activation de la solution MDR à l'aide d'un fichier clé et d'un code d'activation.
Kaspersky Endpoint Security for Mac	12.2 ou version ultérieure 	12-12.1 	Kaspersky Endpoint Security for Mac prend en charge l'activation de la solution MDR à l'aide d'un code d'activation.
Kaspersky Security for Virtualization Light Agent	6.3 ou version ultérieure 	5.2-6.2 	Pour en savoir plus, consultez l'article suivant : Versions prises en charge des applications en mode Light Agent .
Kaspersky Embedded Systems Security for Windows	4.0 ou version ultérieure 	4.0 	Kaspersky Endpoint Security for Windows prend en charge l'activation de la solution MDR à l'aide d'un fichier clé et d'un code d'activation.
Kaspersky Embedded Systems Security for Linux	4.0 ou version ultérieure 	4.0 	Kaspersky Embedded Systems Security for Linux prend en charge l'activation de la solution MDR à l'aide d'un fichier clé et d'un code d'activation.
Kaspersky Industrial CyberSecurity for Nodes Windows	4.5 	4.5 	Utilisez le plug-in MDR version 3.0.0 ou une version ultérieure pour appliquer plusieurs codes d'activation pour la licence Kaspersky Industrial CyberSecurity for Nodes. Vous pouvez utiliser la Console MDR en ligne si vous ne disposez que d'un code d'activation unique pour la licence Kaspersky Industrial CyberSecurity for Nodes. L'application des nouveaux codes d'activation pour Kaspersky Industrial CyberSecurity for Nodes n'est pas disponible dans la région du Royaume d'Arabie saoudite, si vous possédez l'une des licences suivantes : • Module complémentaire pour Kaspersky Managed Detection and Response Basic • Module complémentaire pour Kaspersky Managed Detection and Response Advanced • Module complémentaire pour Kaspersky Managed Detection and Response Prime
Kaspersky Endpoint Agent	-	4.0 ou version ultérieure 	Nous vous recommandons de passer à Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Agent est utilisé uniquement si vous utilisez Kaspersky Security for Windows Server.

* L'intégration MDR est disponible avec certaines limitations fonctionnelles (par exemple, une télémétrie réduite ou un nombre inférieur d'actions de réponse automatisées).

Pour en savoir plus sur les versions prises en charge des applications et des solutions Kaspersky, consultez la [page Internet du cycle de vie de l'assistance produit](#).

Pour en savoir plus sur l'intégration à d'autres solutions Kaspersky, consultez l'article suivant : [Intégration aux applications et aux solutions Kaspersky](#).

Kaspersky Security Center

Le tableau ci-dessous répertorie les composants de Kaspersky Security Center pris en charge par la solution MDR.

Composants de Kaspersky Security Center	Versions et leur durée de prise en charge	Remarques
Kaspersky Security Center Windows	15.1 ou version ultérieure	Utilisé avec le plug-in MDR pour Kaspersky Security Center .
Kaspersky Security Center Linux	15.1 ou version ultérieure	Utilisé avec le plug-in MDR pour Kaspersky Security Center .
Kaspersky Next Expert View	Expert View	
Plug-in MDR pour Kaspersky Security Center	Dernière version	La version 2.5.1 est la version minimale prise en charge.

Console MDR en ligne

La Console MDR en ligne requiert la configuration matérielle et logicielle suivante :

- Moniteur prenant en charge une résolution d'affichage de 1 024 x 768 ou supérieure
- L'un des navigateurs suivants :
 - Apple Safari : version 18.3 ou ultérieure sous macOS
 - Google Chrome : 143.0.7499.40 ou version ultérieure (build officiel)
 - Microsoft Edge : 143.0.3650.66 ou version ultérieure
 - Mozilla Firefox Extended Support Release : 140.5.0.2342 ou version ultérieure

Canal réseau

Le tableau suivant affiche le débit du canal du réseau calculé à partir de nos données statistiques.

Système opérateur	Bande passante estimée pour 1 000 ressources
Windows	4,3 Mbit/s
Windows Server	5,2 Mbit/s

Système opérateur	Bande passante estimée pour 1 000 ressources
Linux (moyenne pour les hôtes et les serveurs)	14,7 Mbit/s
macOS	8,5 Mbit/s

Ces valeurs de bande passante sont approximatives, car la bande passante nécessaire dépend fortement du type de charge de la ressource générant des événements de télémétrie. Le débit maximal peut être nettement plus élevé. Une bande passante réseau plus élevée sera nécessaire si votre infrastructure fonctionne régulièrement à un débit maximal. Diverses conditions peuvent supposer que la charge est plus élevée. Par exemple :

- compilation du code du programme par les développeurs
- analyse complète du système
- serveurs à charge élevée (par exemple, DNS et contrôleurs de domaine)
- connexions réseau multiples

Fonctionnalité des versions du plug-in MDR et compatibilité avec Kaspersky Security Center et Open Single Management Platform

Le tableau ci-dessous indique les versions de Kaspersky Security Center et Open Single Management Platform compatibles avec les versions du plug-in MDR.

Fonctionnalité des versions du plug-in MDR et compatibilité avec Kaspersky Security Center

Version du plug-in MDR	Version compatible de Kaspersky Security Center	Fonctionnalités ajoutées dans la version du plug-in MDR
2.5.1	Kaspersky Security Center Windows version 15.1 ou ultérieure Kaspersky Security Center Windows Linux version 16.1 ou ultérieure	Utilisation de plusieurs clés de licence. Possibilité de générer un fichier de configuration MDR (BLOB) pour une clé de licence spécifique. Configuration des actions de réponse automatiques pour les locataires. Rapports configurables spécifiques aux locataires.
2.5.2	Kaspersky Security Center Windows version 15.1 ou ultérieure Kaspersky Security Center Windows Linux version 16.1 ou ultérieure	Fonctionnement sans fichiers de configuration KPSN.
3.0.0	Kaspersky Security Center Windows version 15.1 ou ultérieure Kaspersky Security Center Windows Linux version 16.1 ou ultérieure	Prise en charge des applications EPP suivantes : • Kaspersky Industrial CyberSecurity for Nodes Windows – version 4.5 ou ultérieure • Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure
3.1.0	Kaspersky Security Center Windows version 15.1 ou ultérieure Kaspersky Security Center Windows Linux version 16.1 ou ultérieure	Prise en charge des applications EPP suivantes : • Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure Possibilité d'indiquer la limite de ressources pour les locataires. À partir de la version 3.1.0 du plug-in MDR, les notifications ne peuvent plus être configurées dans Kaspersky Security Center. Utilisez la Console MDR en ligne pour configurer les notifications.

Version du plug-in MDR	Version compatible d'Open Single Management Platform	Fonctionnalités ajoutées dans la version du plug-in MDR
3.0.1	2.0	Intégration de Kaspersky Endpoint Detection and Response Expert : - Création d'incidents MDR à partir d'incidents EDR. - L'action de réponse Get artefacts, qui permet de copier les fichiers relatifs aux alertes ou aux incidents de Kaspersky EDR vers Kaspersky SOC. La prise en charge de la version 2.0 d'Open Single Management Platform est limitée à la version 3.0.1 du plug-in MDR.
3.0.2	2.1	Intégration de MDR avec Open Single Management Platform version 2.1.
3.1.0	2.1	Prise en charge des applications EPP suivantes : Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure Possibilité d'indiquer la limite de ressources pour les locataires. À partir de la version 3.1.0 du plug-in MDR, les notifications ne peuvent plus être configurées dans Open Single Management Platform. Utilisez la Console MDR en ligne pour configurer les notifications.
3.1.1	2.2	Intégration de MDR avec Open Single Management Platform version 2.2.

Modules de Kaspersky Managed Detection and Response

Description des composants de Kaspersky Managed Detection and Response :

- Une [ressource](#) désigne un appareil d'une organisation qui est protégé par les solutions Kaspersky.
- L'application EPP est une application Kaspersky qui protège les ressources et les données qui y sont stockées contre les applications malveillantes et les autres menaces.
- Kaspersky Endpoint Agent est un composant de programme installé sur les postes de travail et les serveurs de l'infrastructure informatique de l'entreprise. Kaspersky Endpoint Agent surveille en permanence les processus exécutés sur ces ordinateurs, les connexions réseau actives et les fichiers modifiés. Dans les versions récentes des applications EPP, il a été remplacé par la fonctionnalité intégrée.
- L'Agent d'administration de Kaspersky est un composant de Kaspersky Security Center qui permet l'interaction entre le serveur d'administration et les applications Kaspersky installées sur un nœud de réseau spécifique (poste de travail ou serveur). Ce composant est commun à toutes les applications de l'entreprise pour Microsoft Windows. Des versions distinctes de l'Agent d'administration existent pour les applications Kaspersky développées pour les systèmes d'exploitation de type Unix et macOS.
- Kaspersky Security Center est une application destinée aux administrateurs de réseau d'entreprise et aux employés responsables de la protection des ressources dans un large éventail d'organisations.
- Kaspersky Security Network est une infrastructure de services cloud qui permet d'accéder à la base de connaissances en ligne de Kaspersky, qui contient des informations sur la réputation des fichiers, des ressources Internet et des logiciels. L'utilisation des données de Kaspersky Security Network garantit des réponses plus rapides des applications Kaspersky aux menaces, améliore les performances de certains composants de protection et réduit la probabilité de fausses alarmes.
- Le service Kaspersky Managed Detection and Response (également appelé MDR) est une solution qui offre une protection gérée en continu, permettant aux entreprises de détecter automatiquement les menaces évanescentes, tout en permettant aux équipes de sécurité informatique de se concentrer sur ces tâches critiques qui requièrent leur attention.

- La Console MDR en ligne fournit une interface Web pour la gestion et la maintenance du système de protection du réseau d'une organisation cliente géré par Kaspersky Managed Detection and Response. En plus de la Console MDR en ligne, le plug-in Web de Kaspersky Security Center a été ajouté pour permettre la gestion de Kaspersky Managed Detection and Response au sein d'une console d'administration unique.
- L'API MDR est l'interface de programmation d'applications permettant de gérer et de prendre en charge le système de protection du réseau d'une organisation cliente gérée par Kaspersky Managed Detection and Response.

Activation et déploiement de Kaspersky Managed Detection and Response

Cette section décrit comment activer et déployer Kaspersky Managed Detection and Response.

Pour activer et déployer Kaspersky Managed Detection and Response, vous avez besoin de l'une des solutions d'administration centralisée de la sécurité du réseau suivantes :

- Sur site : [Kaspersky Security Center Web Console](#) [☞], [Open Single Management Platform](#) [☞].
- Dans le Cloud : [Kaspersky Next Expert View](#) [☞].

Les étapes du déploiement de Kaspersky Managed Detection and Response dépendent des [applications EPP](#) [☞] spécifiques qui sont installées sur vos ressources et de l'utilisation de la [multilocation](#).

Versions à jour des applications, locataire unique

[Activez et déployez MDR en utilisant uniquement des applications à jour et un locataire unique](#) si les conditions suivantes sont remplies :

- Des versions à jour des applications sont installées sur toutes vos ressources :
 - Kaspersky Endpoint Security for Windows – version 12.10 ou ultérieure
 - Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
 - Kaspersky Endpoint Security for Mac – version 12.2 ou ultérieure
 - Kaspersky Industrial CyberSecurity for Nodes Windows – version 4.5 ou ultérieure
 - Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure
 - Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure
- Vous ne prévoyez pas de configurer la multilocation immédiatement après le déploiement. Vous pouvez configurer la multilocation ultérieurement.
- Vous possédez l'une des licences suivantes :
 - Kaspersky Next Complete Security
 - Kaspersky Optimum Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Versions à jour des applications, multilocation

Activez et déployez MDR en utilisant uniquement des applications à jour et la multilocation si les conditions suivantes sont remplies :

- Des versions à jour des applications sont installées sur toutes vos ressources :
 - Kaspersky Endpoint Security for Windows – version 12.10 ou ultérieure
 - Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
 - Kaspersky Endpoint Security for Mac – version 12.2 ou ultérieure
 - Kaspersky Industrial CyberSecurity for Nodes Windows – version 4.5 ou ultérieure
- Vous prévoyez de configurer la multilocation immédiatement après le déploiement.
- Vous possédez l'une des licences suivantes :
 - Kaspersky Next Complete Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response
 - Module complémentaire pour Kaspersky MDR Expert
 - Module complémentaire pour Kaspersky MDR Optimum
 - Module complémentaire pour Kaspersky Managed Detection and Response Basic
 - Module complémentaire pour Kaspersky Managed Detection and Response Advanced
 - Module complémentaire pour Kaspersky Managed Detection and Response Prime

Anciennes versions des applications

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

[Activez et déployez MDR si votre infrastructure comprend des ressources avec des versions héritées d'applications](#) :

- Kaspersky Endpoint Security for Windows version 12.9 ou version antérieure
- Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure
- Kaspersky Endpoint Security for Mac version 12.1 ou version antérieure
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server avec Kaspersky Endpoint Agent for Windows

Composants nécessaires au fonctionnement de la solution MDR

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Le tableau ci-dessous répertorie les composants requis pour l'envoi de télémétrie à partir des ressources. Si l'un de ces composants est désactivé ou manquant, Kaspersky Managed Detection and Response interrompt l'envoi de télémétrie à partir de la ressource.

Le mode Light Agent est pris en charge pour les versions suivantes :

- Kaspersky Endpoint Security for Windows – version 12.8 ou ultérieure
- Kaspersky Endpoint Security for Linux – version 12.1 ou ultérieure

Module	Documentation
Détection comportementale	Kaspersky Endpoint Security for Windows  Kaspersky Endpoint Security for Linux  Kaspersky Embedded Systems Security for Windows  Kaspersky Embedded Systems Security for Linux  Kaspersky Industrial CyberSecurity for Nodes 

Module	Documentation
Protection contre les fichiers malicieux	Kaspersky Endpoint Security for Windows  Kaspersky Endpoint Security for Linux  Kaspersky Endpoint Security for Mac  Kaspersky Security for Virtualization Light Agent  Kaspersky Embedded Systems Security for Windows  Kaspersky Embedded Systems Security for Linux  Kaspersky Industrial CyberSecurity for Nodes 
Surveillance du système	Kaspersky Security for Virtualization Light Agent 

Le tableau ci-dessous dresse la liste des modules qui ont une incidence sur toutes les données télémétriques envoyées.

Module	Documentation
Pare-feu	Kaspersky Endpoint Security for Windows  Kaspersky Security for Virtualization Light Agent  Kaspersky Embedded Systems Security for Windows  Kaspersky Industrial CyberSecurity for Nodes 
Protection contre les menaces réseau	Kaspersky Endpoint Security for Windows  Kaspersky Endpoint Security for Linux  Kaspersky Endpoint Security for Mac  Kaspersky Embedded Systems Security for Windows  Kaspersky Embedded Systems Security for Linux  Kaspersky Industrial CyberSecurity for Nodes 
Protection contre les menaces par emails	Kaspersky Endpoint Security for Windows 
Protection contre les menaces Internet	Kaspersky Endpoint Security for Windows  Kaspersky Endpoint Security for Linux  Kaspersky Endpoint Security for Mac  Kaspersky Embedded Systems Security for Linux  Kaspersky Security for Virtualization Light Agent 
Autodéfense	Kaspersky Endpoint Security for Windows  Kaspersky Security for Virtualization Light Agent  Kaspersky Embedded Systems Security for Windows  Kaspersky Industrial CyberSecurity for Nodes 

Intégration avec les applications et solutions Kaspersky

Le tableau ci-dessous décrit comment configurer l'intégration de Kaspersky Managed Detection and Response avec les autres solutions et applications Kaspersky.

Solution ou application	Version	Configuration
Kaspersky Endpoint Security for Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security for Mac Kaspersky Security for Virtualization Light Agent Kaspersky Industrial CyberSecurity for Nodes Windows Kaspersky Embedded Systems Security Windows Kaspersky Security for Windows Server avec Kaspersky Endpoint Agent for Windows		Consultez l'article suivant : Activation de la solution MDR dans les applications Kaspersky .
Kaspersky Endpoint Detection and Response Expert (on-premise)	8.0 ou version ultérieure intégrée à Open Single Management Platform avec Kaspersky Next XDR 2.1 ou version ultérieure	Requiert des clés de licence actives pour Kaspersky MDR Expert et Kaspersky EDR Expert. Le rôle Administrateur MDR est requis pour la configuration de l'intégration. 1. Configurez le plug-in MDR dans Open Single Management Platform Console. 2. Dans la section MDR de l'interface de la Console OSMP, cliquez sur l'onglet Utilisation de MDR. 3. Développez le groupe fichier de configuration KPSN pour l'intégration avec KEDR Expert. 4. Activez l'option Accepter le contrat KPSN et cliquez sur Appliquer le fichier de configuration KPSN pour l'intégration avec KEDR Expert. La solution MDR reçoit désormais des données télémétriques comprenant des alertes KEDR à des fins d'analyse.
Kaspersky Unified Monitoring and Analysis Platform	4.0 ou version ultérieure	Consultez l'article suivant : Intégration à Kaspersky Managed Detection and Response .
Kaspersky Anti Targeted Attack (KATA) Platform	7.0–7.1	1. Téléchargez le fichier de configuration MDR. 2. Activez l'intégration MDR. Non disponible dans la région suivante : Royaume d'Arabie saoudite.
	8.0 ou version ultérieure	Assurez-vous que le serveur sur lequel la configuration avec la solution MDR est effectuée dispose d'un accès réseau aux adresses suivantes : • *uis.kaspersky.com:443 • mdr.kaspersky.com:443 Assurez l'accès réseau des serveurs KATA secondaires à l'adresse mdr.kaspersky.com:443. Consultez l'article suivant : Configuration de l'intégration à Kaspersky Managed Detection and Response . Non disponible dans la région suivante : Royaume d'Arabie saoudite.

Configuration du plug-in MDR

Pour administrer Kaspersky Managed Detection and Response via la fonctionnalité du plug-in MDR, vous devez installer le plug-in MDR dans la solution d'administration centralisée de la sécurité du réseau que vous utilisez :

- Kaspersky Security Center Web Console
- Kaspersky Next Expert View

Le plug-in MDR est préinstallé dans Kaspersky Next Expert View.

- Open Single Management Platform

Conditions préalables

Assurez-vous d'avoir accès à Kaspersky Security Center Web Console, à Kaspersky Next Expert View ou à Open Single Management Platform avec les droits d'accès minimaux suivants :

- Droit d'accès en **lecture** au domaine fonctionnel [Fonctionnalités générales : Intégration des applications](#)
- **Autoriser** l'accès au domaine fonctionnel [Accès aux incidents](#) de Kaspersky Managed Detection and Response

Installation du plug-in MDR dans Kaspersky Security Center Web Console

Pour installer le plug-in MDR dans Kaspersky Security Center Web Console, procédez comme suit :

1. Dans le menu principal de Kaspersky Security Center Web Console, accédez à **Paramètres** → **Plug-ins Web**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.
Une liste des plug-ins disponibles s'affiche.
3. Dans la liste des plug-ins disponibles, sélectionnez le plug-in MDR.
La page de description du plug-in s'affiche.
4. Sur la page de description du plug-in, cliquez sur **Installer le plug-in**.
5. Une fois l'installation terminée, cliquez sur **OK**.

Le plug-in MDR est téléchargé avec la configuration par défaut et s'affiche dans la liste des plug-ins Internet d'administration.

Installation du plug-in MDR dans Open Single Management Platform

Si Open Single Management Platform fonctionne dans un environnement réseau fermé, vous devez spécifier les paramètres du serveur proxy. Exécutez la commande suivante sur l'hôte d'Open Single Management Platform pour ajouter des variables d'environnement contenant les paramètres du serveur proxy :

```
kubectl set env deployment/plugin-mdr-proxy -n nwc \
  HTTP_PROXY=http://<proxy>:8080 \
  HTTPS_PROXY=http://<proxy>:8080 \
  NO_PROXY=localhost,127.0.0.1,.local,.cluster.local
```

Exécutez la commande suivante pour vérifier que les variables d'environnement ont été configurées :

```
kubectl rollout status deployment/plugin-mdr-proxy -n nwc
```

Pour installer le plug-in MDR dans OSMP, procédez comme suit :

1. Déplacez l'archive du plug-in d'administration vers l'hôte administrateur sur lequel se trouve l'utilitaire KDT.
2. Sur l'hôte administrateur avec l'utilitaire KDT, exécutez la commande suivante pour installer le plug-in :

```
./kdt apply -k <chemin d'accès à l'archive du plug-in>
```

3. Rechargez l'interface de la console OSMP pour afficher le plug-in ajouté.

Le plug-in d'administration de MDR est installé, et vous pouvez accéder aux fonctions de MDR dans la console OSMP.

Vous pouvez utiliser l'utilitaire KDT pour afficher la liste des plug-ins Internet installés et vous assurer que le plug-in d'administration de MDR a été installé correctement.

Pour afficher la liste des plug-ins d'administration et autres modules liés à OSMP,

Sur l'hôte administrateur sur lequel se trouve l'utilitaire KDT, exécutez la commande suivante :

```
./kdt state
```

La liste des modules intégrés dans OSMP s'affiche dans la fenêtre de ligne de commande. Vous pouvez vérifier la liste pour vous assurer que le plug-in d'administration de MDR a bien été installé.

Résultats

Une fois ce scénario terminé, le plug-in MDR est configuré pour fonctionner avec Kaspersky Managed Detection and Response.

Activation et déploiement de MDR en cas d'utilisation de versions à jour des applications et d'un locataire unique

La procédure suivante, qui décrit l'activation et le déploiement de la solution MDR, s'applique si les conditions suivantes sont remplies :

- Des versions à jour des applications sont installées sur toutes vos ressources :
 - Kaspersky Endpoint Security for Windows – version 12.10 ou ultérieure
 - Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
 - Kaspersky Endpoint Security for Mac – version 12.2 ou ultérieure
 - Kaspersky Industrial CyberSecurity for Nodes Windows – version 4.5 ou ultérieure
 - Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure
 - Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure
- Vous ne prévoyez pas d'utiliser la [multilocation](#) immédiatement après le déploiement.
Vous pourrez configurer la multilocation ultérieurement en ajoutant des fichiers de configuration MDR (BLOB) aux applications.
- Vous possédez l'une des licences suivantes :
 - Kaspersky Next Complete Security
 - Kaspersky Optimum Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response

Conditions préalables

Assurez-vous que votre infrastructure informatique répond aux [exigences matérielles et logicielles de Kaspersky Managed Detection and Response](#).

Activation et déploiement

Pour activer et déployer la solution MDR, procédez comme suit :

Étape 1. Authentification dans la Console MDR en ligne

Procédez comme suit :

1. Accédez à la [Console MDR en ligne](#).
2. Cliquez sur **Créer un compte**. Créez un compte utilisateur.
3. Dans la [Console MDR en ligne](#), connectez-vous avec le compte utilisateur créé.
4. Lorsque vous y êtes invité, saisissez le code d'activation envoyé à l'adresse email que vous avez indiquée lors de la création de votre compte utilisateur.
5. Sélectionnez la région de traitement des données en fonction du lieu d'utilisation de la licence.
6. Lorsque vous y êtes invité, acceptez les accords et confirmez l'activation de MDR.

Étape 2. Activation de la solution MDR sur vos ressources

Si vous utilisez la solution MDR avec l'une des licences suivantes, la solution MDR est automatiquement activée sur vos ressources. Vous pouvez donc ignorer cette étape et passer à l'étape 3 :

- Kaspersky Next Complete Security
- Kaspersky Symphony MDR
- Kaspersky Next MDR Optimum

Activez la licence MDR sur vos ressources :

Activation dans Kaspersky Security Center Web Console

1. Dans le menu principal, accédez à **Opérations** → **Licences pour les logiciels de Kaspersky**.
2. Cliquez sur le bouton **Ajouter**.
3. Ajoutez le fichier clé ou appliquez le code d'activation :
 - **Ajouter un fichier clé**
Cliquez sur le bouton **Sélectionner le fichier clé** et recherchez le fichier .key que vous souhaitez ajouter.

- **Saisir un code d'activation**

Saisissez le code d'activation et cliquez sur le bouton **Envoyer**.

4. Cliquez sur le bouton **Fermer**.

5. Sur la page **Licences pour les logiciels de Kaspersky**, cliquez sur le nom de la licence actuelle.

La page des propriétés de la licence s'ouvre.

6. Sous l'onglet **Général**, activez le paramètre **Distribuer automatiquement la clé de licence sur les appareils administrés**.

7. Cliquez sur **Enregistrer**.

La clé de licence est automatiquement distribuée aux ressources. Si vous souhaitez diffuser une clé de licence sur les appareils clients via la tâche de diffusion de la clé de licence, consultez l'[aide en ligne de Kaspersky Security Center](#).

Activation dans Open Single Management Platform

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.

La fenêtre des propriétés du Serveur d'administration s'ouvre.

2. Sous l'onglet **Général**, sélectionnez la section **Clés de licence**.

3. Cliquez sur **Ajouter une nouvelle clé de licence** et indiquez une nouvelle clé de licence.

4. Cliquez sur **Enregistrer**.

5. Sur la page **Clés de licence**, cliquez sur le nom de la clé de licence ajoutée.

La page des propriétés de la clé de licence s'ouvre.

6. Sous l'onglet **Général**, activez le paramètre **Distribuer automatiquement la clé de licence sur les appareils administrés**.

7. Cliquez sur **Enregistrer**.

La clé de licence est automatiquement distribuée aux ressources.

L'article suivant explique comment afficher les clés de licence et les codes d'activation utilisés sur le Serveur d'administration : [Affichage des informations sur les clés de licence et les codes d'activation utilisés](#).

Étape 3. Activation de l'utilisation de KSN

Dans Kaspersky Security Center Web Console, Kaspersky Next Expert View ou Open Single Management Platform, accédez à la section **Administration des ressources** → **Stratégies et profils**. Activez l'utilisation de KSN dans les stratégies pour toutes les applications utilisées sur vos ressources :

Kaspersky Endpoint Security for Windows/Linux

1. Sélectionnez la stratégie de l'application. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
2. Dans les paramètres de stratégie de l'application, accédez à **Paramètres de l'application** → **Paramètres généraux** → **Kaspersky Security Network**.
3. Activez le paramètre **Utilisation de Kaspersky Security Network**.
4. Activez le paramètre **Utiliser le mode KSN étendu**.
5. Si vous souhaitez utiliser le Serveur d'administration en tant que proxy, activez les paramètres suivants :
 - **Utiliser le Serveur d'administration en tant que serveur proxy KSN** pour envoyer la télémétrie des ressources via le proxy KSN.
 - **Utiliser les serveurs Kaspersky Security Network en cas d'indisponibilité du serveur proxy KSN** pour envoyer la télémétrie des ressources via KSN lorsque le proxy KSN n'est pas disponible.
6. Cliquez sur **Enregistrer et fermer**.

Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct. Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Kaspersky Endpoint Security for Mac

1. Sélectionnez la stratégie de l'application. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
2. Dans les paramètres de stratégie de l'application, accédez à **Paramètres de l'application** → **Protection avancée contre les menaces** → **Kaspersky Security Network**.
3. Activez le paramètre **Kaspersky Security Network**.
4. Activez le paramètre **Mode KSN étendu**.
5. Si vous souhaitez utiliser le Serveur d'administration en tant que proxy, activez les paramètres suivants :
 - **Utiliser le Serveur d'administration en tant que serveur proxy KSN** pour envoyer la télémétrie des ressources via le proxy KSN.
 - **Utiliser les serveurs Kaspersky Security Network en cas d'indisponibilité du serveur proxy KSN** pour envoyer la télémétrie des ressources via KSN lorsque le proxy KSN n'est pas disponible.
6. Cliquez sur **Enregistrer et fermer**.

Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct. Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Étape 4. Configuration des paramètres réseau de vos ressources

Pour les ressources disposant d'un accès à Internet, autorisez le trafic sortant non SSL et désactivez l'inspection du trafic sur les ports 443 et 1443 vers les adresses suivantes :

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Pour les ressources sans accès à Internet, configurez KSN Proxy afin qu'elles puissent accéder aux serveurs KSN. Autorisez le trafic sortant non SSL et désactivez l'inspection du trafic pour les variantes suivantes :

- Trafic de la ressource vers KSN Proxy via le port 13111 ([port par défaut](#)).
- Trafic provenant du proxy KSN via les ports 443 et 1443 vers les adresses suivantes :

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Nous vous recommandons de configurer une connexion directe entre les ressources et les serveurs KSN. Cette approche permet d'éviter les pertes de données télémétriques en cas d'indisponibilité du proxy KSN ou pour les ordinateurs portables qui utilisent une connexion à distance.

La solution MDR a été activée et déployée. Les ressources administrées par MDR sont affichées dans la Console MDR en ligne après la synchronisation (jusqu'à 24 heures) : mdr.kaspersky.com/assets.

Vous pouvez maintenant procéder à la configuration de la solution MDR :

- [Invitez de nouveaux utilisateurs dans la Console MDR en ligne.](#)
- [Configurez les notifications standard.](#)
- [Activez les notifications détaillées.](#)

Activation et déploiement de MDR en cas d'utilisation de versions à jour des applications et de la multilocation

La procédure suivante, qui décrit l'activation et le déploiement de la solution MDR, s'applique si les conditions suivantes sont remplies :

- Des versions à jour des applications sont installées sur toutes vos ressources :
 - Kaspersky Endpoint Security for Windows – version 12.10 ou ultérieure
 - Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
 - Kaspersky Endpoint Security for Mac – version 12.2 ou ultérieure
 - Kaspersky Industrial CyberSecurity for Nodes Windows – version 4.5 ou ultérieure
 - Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure (ne peut être attribué qu'au locataire racine)
 - Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure (ne peut être attribué qu'au locataire racine)
- Vous prévoyez d'utiliser la [multilocation](#) immédiatement après le déploiement.
- Vous possédez l'une des licences suivantes :
 - Kaspersky Next Complete Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response
 - Module complémentaire pour Kaspersky MDR Expert
 - Module complémentaire pour Kaspersky MDR Optimum
 - Module complémentaire pour Kaspersky Managed Detection and Response Basic
 - Module complémentaire pour Kaspersky Managed Detection and Response Advanced
 - Module complémentaire pour Kaspersky Managed Detection and Response Prime

Conditions préalables

Assurez-vous que votre infrastructure informatique répond aux [exigences matérielles et logicielles de Kaspersky Managed Detection and Response](#).

Activation et déploiement

Pour activer et déployer la solution MDR, procédez comme suit :

Étape 1. Authentification dans la Console MDR en ligne

Procédez comme suit :

1. Accédez à la [Console MDR en ligne](#).
2. Cliquez sur **Créer un compte**. Créez un compte utilisateur.
3. Dans la [Console MDR en ligne](#), connectez-vous avec le compte utilisateur créé.
4. Lorsque vous y êtes invité, saisissez le code d'activation envoyé à l'adresse email que vous avez indiquée lors de la création de votre compte utilisateur.
5. Sélectionnez la région de traitement des données en fonction du lieu d'utilisation de la licence.
6. Lorsque vous y êtes invité, acceptez les accords et confirmez l'activation de MDR.

Étape 2. Création de locataires et téléchargement des fichiers de configuration

Suivez les instructions ci-dessous :

1. [Créez de nouveaux locataires dans la Console MDR en ligne](#).
2. Pour chacun des locataires créés, [téléchargez le fichier de configuration MDR et ajoutez le fichier BLOB \(P7\) aux stratégies de l'application](#).

Étape 3. Activation de la solution MDR sur vos ressources

Si vous utilisez la solution MDR avec l'une des licences suivantes, la solution MDR est automatiquement activée sur vos ressources. Vous pouvez donc ignorer cette étape et passer à l'étape 4 :

- Kaspersky Next Complete Security
- Kaspersky Symphony MDR
- Kaspersky Next MDR Optimum

Activez la licence MDR sur vos ressources :

Activation dans Kaspersky Security Center Web Console

1. Dans le menu principal, accédez à **Opérations** → **Licences pour les logiciels de Kaspersky**.
2. Cliquez sur le bouton **Ajouter**.
3. Ajoutez le fichier clé ou appliquez le code d'activation :
 - **Ajouter un fichier clé**
Cliquez sur le bouton **Sélectionner le fichier clé** et recherchez le fichier .key que vous souhaitez ajouter.
 - **Saisir un code d'activation**
Saisissez le code d'activation et cliquez sur le bouton **Envoyer**.
4. Cliquez sur le bouton **Fermer**.
5. Sur la page **Licences pour les logiciels de Kaspersky**, cliquez sur le nom de la licence actuelle.
La page des propriétés de la licence s'ouvre.
6. Sous l'onglet **Général**, activez le paramètre **Distribuer automatiquement la clé de licence sur les appareils administrés**.
7. Cliquez sur **Enregistrer**.

La clé de licence est automatiquement distribuée aux ressources. Si vous souhaitez diffuser une clé de licence sur les appareils clients via la tâche de diffusion de la clé de licence, consultez l'[aide en ligne de Kaspersky Security Center](#).

Activation dans Open Single Management Platform

1. Dans le menu principal, cliquez sur le nom du Serveur d'administration.
La fenêtre des propriétés du Serveur d'administration s'ouvre.
2. Sous l'onglet **Général**, sélectionnez la section **Clés de licence**.
3. Cliquez sur **Ajouter une nouvelle clé de licence** et indiquez une nouvelle clé de licence.
4. Cliquez sur **Enregistrer**.

5. Sur la page **Clés de licence**, cliquez sur le nom de la clé de licence ajoutée.

La page des propriétés de la clé de licence s'ouvre.

6. Sous l'onglet **Général**, activez le paramètre **Distribuer automatiquement la clé de licence sur les appareils administrés**.

7. Cliquez sur **Enregistrer**.

La clé de licence est automatiquement distribuée aux ressources.

L'article suivant explique comment afficher les clés de licence et les codes d'activation utilisés sur le Serveur d'administration : [Affichage des informations sur les clés de licence et les codes d'activation utilisés](#).

Étape 4. Activation de l'utilisation de KSN

Dans Kaspersky Security Center Web Console, Kaspersky Next Expert View ou Open Single Management Platform, accédez à la section **Administration des ressources** → **Stratégies et profils**. Activez l'utilisation de KSN dans les stratégies pour toutes les applications utilisées sur vos ressources :

Kaspersky Endpoint Security for Windows/Linux

1. Sélectionnez la stratégie de l'application. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
2. Dans les paramètres de stratégie de l'application, accédez à **Paramètres de l'application** → **Paramètres généraux** → **Kaspersky Security Network**.
3. Activez le paramètre **Utilisation de Kaspersky Security Network**.
4. Activez le paramètre **Utiliser le mode KSN étendu**.
5. Si vous souhaitez utiliser le Serveur d'administration en tant que proxy, activez les paramètres suivants :
 - **Utiliser le Serveur d'administration en tant que serveur proxy KSN** pour envoyer la télémétrie des ressources via le proxy KSN.
 - **Utiliser les serveurs Kaspersky Security Network en cas d'indisponibilité du serveur proxy KSN** pour envoyer la télémétrie des ressources via KSN lorsque le proxy KSN n'est pas disponible.
6. Cliquez sur **Enregistrer et fermer**.

Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct. Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Kaspersky Endpoint Security for Mac

1. Sélectionnez la stratégie de l'application. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
2. Dans les paramètres de stratégie de l'application, accédez à **Paramètres de l'application** → **Protection avancée contre les menaces** → **Kaspersky Security Network**.

3. Activez le paramètre **Kaspersky Security Network**.

4. Activez le paramètre **Mode KSN étendu**.

5. Si vous souhaitez utiliser le Serveur d'administration en tant que proxy, activez les paramètres suivants :

- **Utiliser le Serveur d'administration en tant que serveur proxy KSN** pour envoyer la télémétrie des ressources via le proxy KSN.
- **Utiliser les serveurs Kaspersky Security Network en cas d'indisponibilité du serveur proxy KSN** pour envoyer la télémétrie des ressources via KSN lorsque le proxy KSN n'est pas disponible.

6. Cliquez sur **Enregistrer et fermer**.

Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct. Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Étape 5. Configuration des paramètres réseau de vos ressources

Pour les ressources disposant d'un accès à Internet, autorisez le trafic sortant non SSL et désactivez l'inspection du trafic sur les ports 443 et 1443 vers les adresses suivantes :

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Pour les ressources sans accès à Internet, configurez KSN Proxy afin qu'elles puissent accéder aux serveurs KSN. Autorisez le trafic sortant non SSL et désactivez l'inspection du trafic pour les variantes suivantes :

- Trafic de la ressource vers KSN Proxy via le port 13111 ([port par défaut](#) [↗]).
- Trafic provenant du proxy KSN via les ports 443 et 1443 vers les adresses suivantes :

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Nous vous recommandons de configurer une connexion directe entre les ressources et les serveurs KSN. Cette approche permet d'éviter les pertes de données télémétriques en cas d'indisponibilité du proxy KSN ou pour les ordinateurs portables qui utilisent une connexion à distance.

La solution MDR a été activée et déployée. Les ressources administrées par MDR sont affichées dans la console MDR après la synchronisation (jusqu'à 24 heures) : mdr.kaspersky.com/assets.

Vous pouvez maintenant procéder à la configuration de la solution MDR :

- [Invitez de nouveaux utilisateurs dans la Console MDR.](#)
- [Configurez les notifications standard.](#)
- [Activez les notifications détaillées.](#)

Activation et déploiement de MDR en cas d'utilisation d'anciennes versions des applications

Suivez les instructions suivantes si votre infrastructure comprend des ressources avec d'anciennes versions d'applications :

- Kaspersky Endpoint Security for Windows version 12.9 ou version antérieure
- Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure
- Kaspersky Endpoint Security for Mac version 12.1 ou version antérieure
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server avec Kaspersky Endpoint Agent for Windows

Conditions préalables

Assurez-vous que votre infrastructure informatique répond aux [exigences matérielles et logicielles de Kaspersky Managed Detection and Response](#).

Activation et déploiement

L'activation et le déploiement de la solution MDR se déroulent par étapes :

Étape 1. Authentification dans la Console MDR en ligne

Procédez comme suit :

1. Accédez à la [Console MDR en ligne](#) [☞].
2. Cliquez sur **Créer un compte**. Créez un compte utilisateur.
3. Dans la [Console MDR en ligne](#) [☞], connectez-vous avec le compte utilisateur créé.

4. Lorsque vous y êtes invité, saisissez le code d'activation envoyé à l'adresse email que vous avez indiquée lors de la création de votre compte utilisateur.
5. Sélectionnez la région de traitement des données en fonction du lieu d'utilisation de la licence.
6. Lorsque vous y êtes invité, acceptez les accords et confirmez l'activation de MDR.

Étape 2. Création de locataires et téléchargement des fichiers de configuration

Suivez les instructions ci-dessous :

1. Si vous avez besoin de la multilocation, [créez de nouveaux locataires dans la Console MDR](#).
2. Pour chacun des locataires créés, [téléchargez le fichier de configuration MDR et ajoutez le fichier BLOB \(P7\) aux stratégies de l'application](#).

Étape 3. Configuration de KPSN

[Déployez le fichier de configuration KPSN](#).

Étape 4. Activation de l'utilisation de KSN

Dans Kaspersky Security Center Web Console, Kaspersky Next Expert View ou Open Single Management Platform, accédez à la section **Administration des ressources** → **Stratégies et profils**. Activez l'utilisation de KSN dans les stratégies pour toutes les applications utilisées sur vos ressources :

1. Sélectionnez la stratégie de l'application. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
2. Dans les paramètres de stratégie de l'application, accédez à **Paramètres de l'application** → **Protection avancée contre les menaces** → **Kaspersky Security Network**.
3. Activez le paramètre **Kaspersky Security Network**.
4. Activez le paramètre **Mode KSN étendu**.
5. (facultatif) Si le Serveur d'administration est utilisé comme proxy, activez les paramètres suivants :
 - Activez l'option **Utiliser le Serveur d'administration en tant que serveur proxy KSN** pour envoyer la télémétrie des ressources via le proxy KSN.
 - Activez l'option **Utiliser les serveurs Kaspersky Security Network si le serveur proxy KSN est indisponible**.
6. Cliquez sur **Enregistrer et fermer**.

Les appareils clients peuvent exécuter les demandes à KSN, obtenir des informations de KSN et transmettre dans KSN les informations même s'ils n'ont pas d'accès Internet direct. Le serveur proxy KSN met en cache les données traitées en diminuant la charge sur le canal du réseau externe et en accélérant l'obtention des informations demandées par l'appareil client.

Étape 5. Configuration des paramètres réseau de vos ressources

Pour les ressources disposant d'un accès à Internet, autorisez le trafic sortant non SSL et désactivez l'inspection du trafic sur les ports 443 et 1443 vers les adresses suivantes :

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Pour les ressources sans accès à Internet, configurez KSN Proxy afin qu'elles puissent accéder aux serveurs KSN. Autorisez le trafic sortant non SSL et désactivez l'inspection du trafic pour les variantes suivantes :

- Trafic de la ressource vers KSN Proxy via le port 13111 ([port par défaut](#)).
- Trafic provenant du proxy KSN via les ports 443 et 1443 vers les adresses suivantes :

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Nous vous recommandons de configurer une connexion directe entre les ressources et les serveurs KSN. Cette approche permet d'éviter les pertes de données télémétriques en cas d'indisponibilité du proxy KSN ou pour les ordinateurs portables qui utilisent une connexion à distance.

La solution MDR a été activée et déployée. Les ressources administrées par MDR seront affichées dans la Console MDR après la synchronisation (jusqu'à 24 heures) : mdr.kaspersky.com/assets.

Vous pouvez maintenant procéder à la configuration de la solution MDR :

- [Invitez de nouveaux utilisateurs dans la Console MDR.](#)
- [Configurez les notifications standard.](#)
- [Activez les notifications détaillées.](#)

Déploiement d'un fichier de configuration KPSN

Vous devez déployer un fichier de configuration KPSN si une ancienne version d'une application est installée sur au moins un élément de votre infrastructure :

- Kaspersky Endpoint Security for Windows version 12.9 ou version antérieure
- Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure
- Kaspersky Endpoint Security for Mac version 12.1 ou version antérieure
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server avec Kaspersky Endpoint Agent for Windows

Le déploiement d'un fichier de configuration KPSN s'effectue en deux étapes.

Étape 1. Téléchargement du fichier de configuration MDR

La procédure de téléchargement du fichier de configuration MDR dépend de la création ou non de locataires supplémentaires et de l'installation ou non du plug-in MDR pour Kaspersky Security Center.

Le fichier de configuration MDR est une archive ZIP contenant un fichier de configuration KPSN (.pkcs7) pour le déploiement des applications EPP.

Pour télécharger le fichier de configuration du MDR dans la Console MDR en ligne, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Settings**.
2. Ouvrez l'onglet **Tenants**.
3. Cliquez sur la ligne contenant le locataire pour lequel vous souhaitez télécharger le fichier de configuration MDR.
Le bloc **Tenant settings** apparaît.
4. Cliquez sur le nom du fichier d'archive pour le télécharger.

Pour télécharger le fichier de configuration MDR dans la console de Kaspersky Security Center, procédez comme suit :

1. Dans la section MDR de Kaspersky Security Center Web Console ou de Kaspersky Next Expert View, cliquez sur **Licences**.
2. Localisez la colonne **Archives pour la configuration des ressources** et cliquez sur le bouton **Télécharger** pour télécharger l'archive.

Étape 2. Déploiement du fichier de configuration KPSN

Vous pouvez déployer le fichier de configuration KPSN dans Kaspersky Security Center Web Console. Si vous avez installé le [plug-in MDR](#), vous pouvez également déployer le fichier de configuration KPSN dans le menu du plug-in MDR.

Décompressez le fichier de configuration MDR et installez le fichier de configuration KPSN (.pkcs7).

Pour installer le fichier de configuration KPSN dans Kaspersky Security Center Web Console, procédez comme suit :

1. Accédez aux propriétés du Serveur d'administration en cliquant sur son nom dans le menu principal.
2. Sous l'onglet **Général**, sélectionnez la section **Paramètres du proxy KSN**.
3. Activez le paramètre **Activer le proxy KSN sur le Serveur d'administration**.
4. Activez le paramètre **Utiliser Kaspersky Private Security Network**.
5. Cliquez sur **Choix du fichier de paramètres de proxy KSN** et chargez le fichier de configuration KPSN (.pkcs7).
Les détails du fichier de configuration KPSN s'affichent.
6. Cliquez sur **Enregistrer**.

Le fichier de configuration KPSN est installé.

Pour installer le fichier de configuration KPSN dans le menu Plug-in MDR de Kaspersky Security Center Web Console ou d'Open Single Management Platform :

1. Dans le menu principal, ouvrez la section **MDR**.
2. Ouvrez l'onglet **Utilisation de MDR**.
3. Développez le bloc **Fichier de configuration KPSN pour l'intégration avec le Serveur d'administration de KSC**.
4. Activez le paramètre **Accepter le contrat KPSN** et cliquez sur **Appliquer le fichier de configuration KPSN sur le Serveur d'administration**.

Le fichier de configuration KPSN est installé.

Déploiement d'un fichier de configuration MDR (BLOB)

Vous pouvez utiliser les fichiers de configuration MDR (BLOB) pour activer la solution MDR dans les applications prenant en charge l'intégration avec MDR via les stratégies de Kaspersky Security Center.

Si vous utilisez des clients autres que le locataire racine, vous devez télécharger les fichiers de configuration MDR pour chaque locataire.

Les anciennes versions des applications nécessitent l'utilisation de fichiers de configuration MDR (BLOB) :

- Kaspersky Endpoint Security for Windows version 12.6 ou version antérieure
- Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure
- Kaspersky Endpoint Security for Mac version 12.1 ou version antérieure
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server avec Kaspersky Endpoint Agent for Windows

L'activation de la solution MDR via le fichier de configuration MDR (BLOB) se déroule en deux étapes.

Étape 1. Téléchargement du fichier de configuration MDR

La procédure de téléchargement du fichier de configuration MDR dépend de la création ou non de locataires supplémentaires et de l'installation ou non du plug-in MDR pour Kaspersky Security Center.

Le fichier de configuration MDR est une archive ZIP contenant un fichier BLOB (P7) destiné au déploiement d'applications EPP.

Pour télécharger le fichier de configuration du MDR dans la Console MDR en ligne, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Settings**.
2. Cliquez sur l'onglet **Tenants**.
3. Cliquez sur la ligne contenant le locataire pour lequel vous souhaitez télécharger le fichier de configuration MDR.

Le bloc **Tenant settings** apparaît.

4. Cliquez sur le nom du fichier d'archive pour le télécharger.

Pour télécharger le fichier de configuration MDR dans la console de Kaspersky Security Center, procédez comme suit :

1. Dans la section MDR de Kaspersky Security Center Web Console ou de Kaspersky Next Expert View, cliquez sur **Licences**.
2. Localisez la colonne **Archives pour la configuration des ressources** et cliquez sur le bouton **Télécharger** pour télécharger l'archive.

Étape 2. Ajout du fichier de configuration MDR (BLOB) aux stratégies d'application

Décompressez le fichier de configuration MDR et utilisez le fichier BLOB (P7) pour activer la solution MDR.

Pour activer la solution MDR dans les applications suivantes :

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac

1. Dans Kaspersky Security Center Web Console ou Open Single Management Platform, accédez à la section **Administration des ressources** → **Stratégies et profils**.
2. Sélectionnez la stratégie de l'application. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à **Agents intégrés** → **Managed Detection and Response**.
5. Activez le paramètre Managed Detection and Response.
6. Cliquez sur **Charger** et sélectionnez le fichier BLOB (P7) que vous avez extrait du fichier de configuration MDR.
7. Fermez l'icône du bouton de verrouillage (🔒) pour appliquer les paramètres.
8. Cliquez sur **Enregistrer et fermer**.

Le fichier de configuration MDR (BLOB) est chargé et automatiquement déployé dans les applications.

Pour activer la solution MDR dans Kaspersky Industrial CyberSecurity for Nodes Windows :

1. Dans Kaspersky Security Center Web Console ou Open Single Management Platform, accédez à la section **Administration des ressources** → **Stratégies et profils**.
2. Sélectionnez la stratégie de Kaspersky Industrial CyberSecurity for Nodes Windows. Si la stratégie de l'application n'a pas été créée, cliquez sur **Ajouter** et créez la stratégie.
3. Sélectionnez l'onglet **Paramètres de l'application**.
4. Accédez à **Serveurs de connexion à la télémétrie**.
5. Dans la section **Managed Detection and Response**, cliquez sur **Configurer**.
6. Activez le paramètre **Managed Detection and Response**.
7. Cliquez sur **Charger** et sélectionnez le fichier BLOB (P7) que vous avez extrait du fichier de configuration MDR.
8. Cliquez sur **Enregistrer et fermer**.

Le fichier de configuration MDR (BLOB) est chargé et automatiquement déployé dans les applications.

Déploiement par capture et copie de l'image d'un appareil

Si vous devez installer des applications sur des ressources sur lesquelles un système d'exploitation et d'autres logiciels doivent également être installés (ou réinstallés), vous pouvez utiliser le mécanisme de capture et de copie de l'image d'une ressource de référence.

Le déploiement par capture et copie de l'image d'un appareil s'effectue en deux étapes :

1. Préparez une ressource de référence sur laquelle les logiciels nécessaires sont installés.
2. Capturez l'image de la ressource de référence préparée et déployez-la sur les équipements à l'aide de la tâche dédiée de Kaspersky Security Center.

Si votre licence Kaspersky Security Center inclut la fonctionnalité de gestion des systèmes, vous pouvez [utiliser cette fonctionnalité pour créer une image et la déployer sur vos ressources](#). Sinon, utilisez les outils tiers disponibles au sein de l'organisation.

Préparation d'une ressource de référence

Pour préparer une ressource de référence sous Windows, procédez comme suit :

1. Installez et configurez le système d'exploitation et les autres logiciels que vous devez distribuer.
2. Sur la ressource de référence, dans les paramètres des connexions réseau de Windows, déconnectez la ressource de référence du réseau sur lequel Kaspersky Security Center est installé.
3. Sur la ressource de référence, lancez l'installation locale de l'Agent d'administration à l'aide du fichier setup.exe.

L'assistant de configuration de l'Agent d'administration de Kaspersky Security Center démarre. Suivez les instructions de l'assistant.

4. Sur la page Serveur d'administration de l'assistant, indiquez l'adresse IP du Serveur d'administration.

Si vous ne connaissez pas l'adresse exacte du Serveur d'administration, saisissez localhost. Vous pouvez modifier l'adresse IP ultérieurement [à l'aide de l'utilitaire klmover](#) avec la clé -address.

5. Sur la page Lancer l'application de l'assistant, désactivez l'option Lancer l'application pendant l'installation.

6. Une fois l'installation de l'Agent d'administration terminée, ne redémarrez pas la ressource avant de créer une image du système d'exploitation.

Si vous redémarrez la ressource, vous devrez répéter l'ensemble du processus de préparation d'une ressource de référence pour la création d'une image du système d'exploitation.

7. Sur la ressource de référence, dans la ligne de commande, lancez l'utilitaire sysprep et exécutez la commande suivante : sysprep.exe /generalize /oobe /shutdown.

La ressource de référence est prête pour la création d'une image du système d'exploitation.

Pour préparer une ressource de référence sous Linux, procédez comme suit :

1. Installez et configurez le système d'exploitation et les autres logiciels que vous devez distribuer.
2. Assurez-vous que les conditions suivantes sont remplies :
 - Kaspersky Endpoint Security for Linux n'est pas installé sur la ressource de référence.
 - L'appareil de référence n'a pas été connecté à Kaspersky Security Center.

Si l'une de ces conditions n'est pas respectée, la solution MDR pourrait ne pas réussir à identifier correctement les ressources créées à partir d'une image de référence. Pour résoudre ce problème, procédez comme suit sur les ressources équipées de Kaspersky Endpoint Security for Linux :

- a. Exécutez les commandes suivantes pour générer un nouvel UUID :

```
uuidgen > /var/opt/kaspersky/kes1/common/pcid  
uuidgen > /var/opt/kaspersky/epagent/install_id
```

- b. Désinstallez Kaspersky Endpoint Security for Linux, puis réinstallez-le.

La ressource de référence est prête pour la création d'une image du système d'exploitation.

Capture et diffusion de l'image d'une ressource de référence

Lorsque vous utilisez des outils tiers pour capturer l'image d'une ressource sur laquelle l'Agent d'administration est installé, procédez de l'une des manières suivantes :

- Méthode recommandée. Lors de l'installation de l'Agent d'administration sur une ressource de référence, capturez l'image de la ressource avant le premier démarrage du service de l'Agent d'administration (car des informations uniques permettant d'identifier la ressource sont créées lors de la première connexion de l'Agent d'administration au Serveur d'administration). Il est ensuite recommandé de ne pas exécuter le service de l'Agent d'administration avant la fin de l'opération de capture d'image.

Pour Windows, consultez l'article suivant : [Préparation d'un élément de référence avec l'Agent d'administration installé pour la création d'une image du système d'exploitation](#) ¹.

Pour Linux, consultez l'article suivant : [Déploiement par capture et copie de l'image d'une ressource](#) ².

- Sur le serveur de référence, arrêtez le service de l'Agent d'administration et exécutez l'utilitaire klmover avec l'option -dupfix. L'utilitaire klmover est inclus dans le paquet d'installation de l'Agent d'administration. Évitez de relancer le service de l'Agent d'administration tant que l'opération de capture d'image n'est pas terminée.

Assurez-vous que l'utilitaire klmover est exécuté avec la clé -dupfix avant le premier démarrage du service de l'Agent d'administration sur les appareils cibles. Cette exigence est obligatoire et doit être respectée lors du premier démarrage du système d'exploitation après le déploiement de l'image.

- Utilisez le mode de clonage de disque de l'Agent d'administration.

Pour Windows, consultez l'article suivant : [Mode de clonage de disque de l'Agent d'administration](#) ³.

Pour Linux, consultez l'article suivant : [Mode de clonage de disque de l'Agent d'administration](#) ⁴.

Vous pouvez également capturer l'image d'une ressource sans installer l'Agent d'administration. Pour ce faire, déployez l'image sur les ressources cibles, puis déployez l'Agent d'administration. Si vous utilisez cette méthode, veillez à ce que les paquets d'installation autonomes soient accessibles depuis le dossier réseau de la ressource. Suivez les instructions :

- Pour Windows, consultez l'article suivant : [Installation d'images de systèmes d'exploitation](#).
- Pour Linux, consultez l'article suivant : [À propos des tâches d'installation à distance dans Kaspersky Security Center pour Linux](#).

Activation de la solution MDR dans les applications Kaspersky

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Cette section contient des informations de référence sur l'activation de la solution MDR en fonction de la licence et des versions des applications. Pour un tutoriel complet sur la manière d'activer la solution MDR, consultez l'article suivant : [Activation et déploiement de Kaspersky Managed Detection and Response](#).

Les articles suivants décrivent comment gérer les clés de licence et les codes d'activation dans le Serveur d'administration :

- [Distribution automatique des clés de licence et des codes d'activation](#)
- [Affichage des informations sur les clés de licence et les codes d'activation utilisés](#)

Licence MDR	Applications prises en charge pour les méthodes suivantes : Code d'activation Fichier BLOB	Applications prises en charge pour les méthodes suivantes : Fichier BLOB
Kaspersky Symphony MDR Kaspersky Next Complete Security Kaspersky Optimum Security Kaspersky Next MXDR Optimum Consultez : licences Kaspersky Symphony MDR et NEXT Complete Security.	• Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure • Kaspersky Endpoint Security for Windows version 12.8 ou ultérieure en mode Light Agent • Kaspersky Endpoint Security for Windows version 12.6 ou ultérieure en mode Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure • Kaspersky Endpoint Security for Linux version 12.3 ou ultérieure en mode Light Agent • Kaspersky Endpoint Security for Mac – version 12.2 ou ultérieure L'installation du fichier BLOB est nécessaire si votre organisation compte plusieurs locaux. L'activation à l'aide d'un fichier clé bénéficie d'une prise en charge limitée. Mer vous recommandons d'utiliser un code d'activation.	• Kaspersky Endpoint Security for Windows version 12.5 ou version antérieure • Kaspersky Endpoint Security for Windows version 5.2–6.1 en mode Light Agent • Kaspersky Endpoint Security for Windows version 12.3–12.5 en mode Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure • Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure en mode Light Agent • Kaspersky Endpoint Security for Mac version 12.1 ou version antérieure Les versions 4.0 à 7.1 de Kaspersky Anti Targeted Attack Platform (y compris EDR) prennent en charge l'installation du fichier de configuration MDR, qui inclut le fichier BLOB et le fichier de configuration KPSN. La version 8.0 de Kaspersky Anti Targeted Attack Platform (y compris EDR) ne requiert pas le fichier de configuration MDR.
Kaspersky MDR Kaspersky Managed Detection and Response Consultez : licences Kaspersky MDR.	• Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure • Kaspersky Endpoint Security for Windows version 12.8 ou ultérieure en mode Light Agent • Kaspersky Endpoint Security for Windows version 12.6 ou ultérieure en mode Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure • Kaspersky Endpoint Security for Linux version 12.3 ou ultérieure en mode Light Agent • Kaspersky Endpoint Security for Mac – version 12.2 ou ultérieure • Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure • Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure L'installation du fichier BLOB est nécessaire si votre organisation compte plusieurs locaux. L'activation à l'aide d'un fichier clé bénéficie d'une prise en charge limitée. Mer vous recommandons d'utiliser un code d'activation.	• Kaspersky Endpoint Security for Windows version 12.5 ou version antérieure • Kaspersky Endpoint Security for Windows version 5.2–6.1 en mode Light Agent • Kaspersky Endpoint Security for Windows version 12.3–12.5 en mode Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure • Kaspersky Endpoint Security for Linux version 12.2 ou version antérieure en mode Light Agent • Kaspersky Endpoint Security for Mac version 12.1 ou version antérieure Les versions 4.0 à 7.1 de Kaspersky Anti Targeted Attack Platform (y compris EDR) prennent en charge l'installation du fichier de configuration MDR, qui inclut le fichier BLOB et le fichier de configuration KPSN.
Module complémentaire pour Kaspersky MDR Optimum Module complémentaire pour Kaspersky MDR Expert Module complémentaire pour Kaspersky Managed Detection and Response Basic Module complémentaire pour Kaspersky Managed Detection and Response Advanced Module complémentaire pour Kaspersky Managed Detection and Response Prime Consultez : licences pour modules complémentaires de Kaspersky MDR.	• Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure • Kaspersky Endpoint Security for Windows version 12.8 ou ultérieure en mode Light Agent • Kaspersky Endpoint Security for Windows version 12.6 ou ultérieure en mode Endpoint Detection and Response Agent L'installation du fichier BLOB est nécessaire si votre organisation compte plusieurs locaux. L'activation à l'aide d'un fichier clé bénéficie d'une prise en charge limitée. Mer vous recommandons d'utiliser un code d'activation.	• Kaspersky Endpoint Security for Windows version 12.5 ou version antérieure • Kaspersky Endpoint Security for Windows version 5.2–6.1 en mode Light Agent • Kaspersky Endpoint Security for Windows version 12.3–12.5 en mode Endpoint Detection and Response Agent Les versions 4.0 à 7.1 de Kaspersky Anti Targeted Attack Platform (y compris EDR) prennent en charge l'installation du fichier de configuration MDR, qui inclut le fichier BLOB et le fichier de configuration KPSN.

Licence MDR	Applications prises en charge pour les méthodes suivantes : Code d'activation Fichier BLOB	Applications prises en charge pour les méthodes suivantes : Fichier BLOB
Kaspersky Managed Detection And Response for Industrial CyberSecurity Consultez : licence pour modules complémentaires de Kaspersky MDR for Industrial CyberSecurity	Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 ou ultérieure. L'installation du fichier BLOB est nécessaire si votre organisation compte plusieurs locataires.	L'installation du fichier BLOB est nécessaire si votre organisation compte plusieurs locataires. Dans ce scénario, le fichier clé ou le code d'activation est toujours nécessaire.

Activation de la solution MDR dans les applications Kaspersky. Licences pour modules complémentaires Kaspersky MDR

Les tableaux ci-dessous décrivent les méthodes d'activation de la solution MDR dans Kaspersky applications pour les licences suivantes :

- Module complémentaire pour Kaspersky MDR Expert
- Module complémentaire pour Kaspersky MDR Optimum
- Module complémentaire pour Kaspersky Managed Detection and Response Basic
- Module complémentaire pour Kaspersky Managed Detection and Response Advanced
- Module complémentaire pour Kaspersky Managed Detection and Response Prime

Kaspersky Endpoint Security for Windows

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.10 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.9	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.6 – 12.8	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.5 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Endpoint Security for Windows en mode Endpoint Detection and Response Agent

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.10 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.9	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB).

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.6 – 12.8	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB).
12.3–12.5	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Security for Virtualization Light Agent

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
6.3 ou version ultérieure Kaspersky Endpoint Security for Windows version 12.10 ou ultérieure en mode Light Agent	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.2 Kaspersky Endpoint Security for Windows 12.8 – 12.9 en mode Light Agent	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
6.3 ou version ultérieure Kaspersky Endpoint Security for Linux version 12.3 ou ultérieure en mode Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne . 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.2 Kaspersky Endpoint Security for Linux 12.2 en mode Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Activation de la solution MDR dans les applications Kaspersky. Licences Kaspersky MDR

Les tableaux ci-dessous décrivent les méthodes d'activation de la solution MDR dans Kaspersky applications pour les licences suivantes :

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Kaspersky Endpoint Security for Windows

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.10 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne . 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.9	Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.6 – 12.8	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.5 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Endpoint Security for Windows en mode Endpoint Detection and Response Agent

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.10 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.9	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB).
12.6 – 12.8	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB).
12.3–12.5	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Security for Virtualization Light Agent

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
6.3 ou version ultérieure Kaspersky Endpoint Security for Windows version 12.10 ou ultérieure en mode Light Agent	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
6.2 Kaspersky Endpoint Security for Windows 12.8 – 12.9 en mode Light Agent	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Pour activer à la fois la solution Endpoint Detection and Response Optimum et la solution MDR, appliquez le code d'activation pour Endpoint Detection and Response Optimum et un fichier de configuration MDR (BLOB) pour la solution MDR.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.
6.3 ou version ultérieure Kaspersky Endpoint Security for Linux version 12.3 ou ultérieure en mode Light Agent	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.2 Kaspersky Endpoint Security for Linux 12.2 en mode Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Endpoint Security for Linux

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.3 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.2 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Endpoint Security for Mac

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.2 ou version ultérieure	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Une configuration MDR (BLOB) expirée doit être remplacée par une nouvelle.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.1 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Embedded Systems Security for Windows

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
4.0	Utilisez un code d'activation ou un fichier clé pour activer la solution MDR. Il n'est pas nécessaire d'utiliser un fichier de configuration MDR (BLOB), car toutes les ressources sont attribuées par défaut au locataire racine.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN.

Kaspersky Embedded Systems Security for Linux

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
4.0	Utilisez un code d'activation ou un fichier clé pour activer la solution MDR. Il n'est pas nécessaire d'utiliser un fichier de configuration MDR (BLOB), car toutes les ressources sont attribuées par défaut au locataire racine.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN.

Activation de la solution MDR dans les applications Kaspersky. Licences Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security et Kaspersky Next MXDR Optimum

Les tableaux ci-dessous décrivent les méthodes d'activation de la solution MDR dans Kaspersky applications pour les licences suivantes :

- Kaspersky Symphony MDR
- Kaspersky Next Complete Security
- Kaspersky Optimum Security
- Kaspersky Next MXDR Optimum

Kaspersky Endpoint Security for Windows

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.10 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.9	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.6 – 12.8	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.5 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Security for Virtualization Light Agent

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
6.0 – 6.1 Kaspersky Security for Virtualization Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.
6.3 ou version ultérieure Kaspersky Endpoint Security for Windows version 12.10 ou ultérieure en mode Light Agent	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Light Agent ne peut pas être activé dans le cadre de la licence NEXT Complete Security.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
6.2 Kaspersky Endpoint Security for Windows 12.8 – 12.9 en mode Light Agent	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment. Light Agent ne peut pas être activé dans le cadre de la licence NEXT Complete Security.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.3 ou version ultérieure Kaspersky Endpoint Security for Linux version 12.3 ou ultérieure en mode Light Agent	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
6.2 Kaspersky Endpoint Security for Linux 12.2 en mode Light Agent	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Endpoint Security for Linux

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.3 ou version ultérieure	Avant d'appliquer un code d'activation ou un fichier clé, vous devez installer le fichier de configuration MDR (BLOB) dans les cas suivants : • Vous utilisez actuellement des locataires MDR. • Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : 1. Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. 2. Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.2 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Kaspersky Endpoint Security for Mac

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
12.2 ou version ultérieure	L'activation de la solution MDR à l'aide d'un fichier clé n'est pas prise en charge. Avant d'appliquer un code d'activation, vous devez installer le Fichier de configuration MDR (BLOB) dans les cas suivants : - Vous utilisez actuellement des locataires MDR. - Vous avez déjà créé des locataires MDR, même si des locataires supplémentaires ont été supprimés. Lorsque vous appliquez un code d'activation, il n'est pas nécessaire de mettre à jour la configuration MDR expirée (BLOB) installée précédemment.	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Pour utiliser la solution MDR sans fichier de configuration KPSN, indiquez le code d'activation même si vous avez déployé un fichier de configuration MDR (BLOB). Si des fichiers de configuration MDR (BLOB) sont déjà installés sur vos ressources et que la solution MDR a été activée avant janvier 2024, il est nécessaire de retélécharger et de réinstaller les fichiers BLOB : - Téléchargez le fichier de configuration MDR (BLOB) pour le locataire requis dans la Console MDR en ligne. - Configurez la stratégie pour installer le fichier BLOB sur vos ressources.
12.1 et versions antérieures	La solution MDR peut être activée avec un fichier de configuration MDR (BLOB).	La solution MDR ne peut fonctionner que si le fichier de configuration KPSN est installé dans Kaspersky Security Center.

Activation de la solution MDR dans les applications Kaspersky. Licence pour le module complémentaire de Kaspersky Managed Detection and Response for Industrial CyberSecurity

Le tableau ci-dessous décrit les méthodes d'activation de la solution MDR dans les applications Kaspersky pour la licence du module complémentaire de Kaspersky Managed Detection and Response for Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Nodes Windows

Version de l'application	Méthode d'activation	Exigences relatives au fichier de configuration KPSN
4.5	Utilisez un code d'activation ou un fichier clé pour activer la solution MDR. - Si vous n'utilisez pas et n'avez jamais créé de locataires MDR, il n'est pas nécessaire d'utiliser un fichier de configuration MDR (BLOB). Si vous utilisez des locataires MDR, vous devez installer un fichier de configuration MDR (BLOB), même s'il a expiré. L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN. Utilisez le plug-in MDR version 3.0.0 ou une version ultérieure pour appliquer plusieurs codes d'activation pour la licence Kaspersky Industrial CyberSecurity for Nodes. Vous pouvez utiliser la Console MDR en ligne si vous ne disposez que d'un code d'activation unique pour la licence Kaspersky Industrial CyberSecurity for Nodes. L'application des nouveaux codes d'activation pour Kaspersky Industrial CyberSecurity for Nodes n'est pas disponible dans la région du Royaume d'Arabie saoudite, si vous possédez l'une des licences suivantes : - Module complémentaire pour Kaspersky Managed Detection and Response Basic - Module complémentaire pour Kaspersky Managed Detection and Response Advanced - Module complémentaire pour Kaspersky Managed Detection and Response Prime	L'application prend en charge l'utilisation de MDR avec ou sans fichier de configuration KPSN.

Licence

Une *licence* est un droit limité dans le temps d'utiliser l'application, accordé en vertu des conditions d'utilisation.

Vous ne pouvez utiliser qu'une seule licence dans la console MDR en ligne et le plug-in MDR version 2.4.1 et les versions antérieures. Lorsque vous saisissez un nouveau code d'activation, il remplace le précédent.

À partir de la version 2.4.2 du plug-in MDR, [vous pouvez utiliser plusieurs licences MDR simultanément](#).

Une licence vous donne droit aux types de services suivants :

- Utilisation de l'application conformément aux conditions d'utilisation
- Accès au support technique

Le volume de services offert et la durée de validité dépendent du type de licence utilisée pour activer l'application.

Les types suivants de licences sont prévus :

- *Évaluation* : une licence gratuite conçue pour découvrir l'application.

La licence d'évaluation présente une courte durée de validité. À l'expiration de la licence d'évaluation, toutes les fonctionnalités de Kaspersky Managed Detection and Response sont désactivées. Pour continuer à utiliser l'application, vous devez acheter une licence commerciale.

Vous pouvez activer l'application à l'aide d'une licence d'évaluation une seule fois uniquement.

- *Commerciale* : une licence payante octroyée à l'achat de l'application.

Lorsque la licence commerciale expire, l'application continue de fonctionner avec des fonctionnalités limitées (la télémétrie n'est pas fournie). Pour continuer à utiliser toutes les fonctionnalités de Kaspersky Managed Detection and Response, vous devez renouveler votre licence commerciale.

Il est conseillé de renouveler la licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre les menaces.

- *Abonnement* : une licence payante qui permet l'utilisation de l'application pour une période de facturation mensuelle ou annuelle, avec renouvellement automatique, jusqu'à annulation ou expiration.

La licence d'abonnement peut être de deux types :

- *Limitée* : renouvelée automatiquement à la fin de chaque période de facturation jusqu'à la date d'expiration définie.
- *Ouverte* : renouvelée automatiquement à la fin de chaque période de facturation jusqu'à l'annulation par le client.

Vous pouvez gérer la licence d'abonnement via Kaspersky License Management Portal (LMP).

Si vous modifiez le champ d'application de votre licence, par exemple, modifiez le nombre de ressources, les détails de la licence sont mis à jour dans la Console MDR en ligne dans les 24 heures.

Lorsque la licence d'abonnement est annulée ou expire, l'application continue de fonctionner avec des fonctionnalités limitées (la télémétrie n'est pas fournie). Pour continuer à utiliser toutes les fonctionnalités de Kaspersky Managed Detection and Response, vous devez renouveler votre licence d'abonnement.

Il est conseillé de renouveler la licence avant sa date d'expiration afin de garantir la protection maximale de l'ordinateur contre les menaces.

Comparatif des niveaux de licence commerciale

L'ensemble des fonctionnalités disponibles dans Kaspersky Managed Detection and Response dépend du niveau de votre licence commerciale (voir le tableau ci-dessous).

Comparaison des niveaux de licence commerciale Kaspersky Managed Detection and Response

Fonctionnalité	MDR / MDR Expert*	MDR Optimum* / MDR Basic*	MDR Advanced*	MDR Prime*
La surveillance, la détection et la gestion des incidents 24 heures sur 24 et 7 jours sur 7	✓	✓	✓	✓
Une détection automatique de menaces	✓	✓	✓	✓
Guides d'intervention et réponse automatique aux incidents	✓	✓	✓	✓
Vérification de l'état et de la visibilité des ressources	✓	✓	✓	✓
La Console MDR en ligne avec des tableaux de bord et des rapports	✓	✓	✓	✓
La capacité d'obtenir des informations avancées sur les incidents	✓	✓	✓	✓
Période de conservation de l'historique des incidents	1 an	1 an	1 an	1 an
Durée de conservation des données brutes	3 mois	1 mois	3 mois	3 mois
La gestion de la détection des menaces et des recherches menées sur les incidents	✓	—	✓	✓
Assistance étendue d'experts pour la gestion des incidents	✓	—	✓	✓
Accès au portail Kaspersky Threat Intelligence (pour les licences dont la date de début est antérieure au 12 juillet 2024)	✓	—	✓	✓
API pour l'exportation des données de Kaspersky MDR	✓	—	✓	✓
Les clients peuvent créer un incident personnalisé qui sera traité par la solution Kaspersky MDR**.	✓	—	✓	✓
Stockage localisé des données*	✓	✓	✓	✓
Multilocation	✓	✓	✓	✓
Ajout et modification de commentaires relatifs aux incidents	✓	✓	✓	✓

Fonctionnalité	MDR / MDR Expert*	MDR Optimum* / MDR Basic*	MDR Advanced*	MDR Prime*
Ajout et modification de pièces jointes relatives aux incidents	✓	✓	✓	✓
Enquête avancée sur les incidents : analyse visant à établir l'historique, les circonstances et le mécanisme détaillé de l'attaque	—	—	✓ Les clients ne peuvent pas choisir les incidents qui feront l'objet d'une enquête approfondie. Le temps de réponse en cas d'incident n'est pas garanti	✓ Les clients peuvent choisir les incidents pour une enquête approfondie (dans la limite de temps achetée). Le temps de réponse en cas d'incident est garanti

* Ce niveau ou cette fonctionnalité est disponible dans certaines régions uniquement et peut ne pas être disponible à l'achat pour les nouveaux clients. Contactez votre fournisseur de solution Kaspersky Managed Detection and Response pour en savoir plus sur les niveaux de licence commerciale qui vous sont proposés.

**La solution Kaspersky Managed Detection and Response assure le traitement de trois demandes par semaine, conformément aux [objectifs de performances de la fourniture de la solution](#). Le nombre de demandes traitées, conformément aux objectifs de performances de la fourniture de la solution, augmente de manière proportionnelle : chaque fois que 10 000 terminaux sont connectés, le nombre de demandes augmente de 1.

A propos du code d'activation

Un *code d'activation* est une suite unique de 20 lettres et nombres. Vous devez saisir un code d'activation afin de pouvoir [activer Kaspersky Managed Detection and Response](#). Vous recevez le code d'activation à l'adresse e-mail que vous avez fournie lors de l'achat de Kaspersky Managed Detection and Response.

Pour activer la solution à l'aide du code d'activation, vous avez besoin d'un accès Internet afin de vous connecter aux serveurs d'activation de Kaspersky.

Si vous avez perdu votre code d'activation, contactez le partenaire Kaspersky auprès duquel vous avez acheté la licence.

Entrez un nouveau code d'activation

Première activation de Kaspersky Managed Detection and Response

Consultez les articles suivants :

- Activation de Kaspersky Managed Detection and Response dans Kaspersky Security Center (recommandé)
- Activation de Kaspersky Managed Detection and Response dans la Console MDR en ligne

Saisie d'un nouveau code d'activation

Vous devez fournir un nouveau code d'activation pour Kaspersky Managed Detection and Response, par exemple, lorsque vous souhaitez mettre à niveau la solution ou lorsque vous devez renouveler votre licence expirée.

Cette fonctionnalité n'est disponible que si vous avez défini le droit d'accès **Intégration d'applications** dans [Kaspersky Security Center Web Console](#) ou [Kaspersky Next Expert View](#).

Pour en savoir plus sur l'administration de plusieurs licences dans Kaspersky Managed Detection and Response dans Kaspersky Security Center avec le plug-in MDR 2.4.2 ou version ultérieure, consultez l'article : [Administration des licences dans Kaspersky Security Center](#).

Si vous utilisez une seule licence pour la solution MDR, vous pouvez renouveler cette licence dans la Console MDR en ligne. Le rôle **Administrateur MDR** est requis.

Si votre organisation dispose de plusieurs licences en cours de validité, vous ne pouvez les gérer que dans Kaspersky Security Center. Dans ce scénario, l'utilisation de la Console MDR en ligne pour le renouvellement de licence entraîne l'arrêt de la transmission des données télémétriques depuis les ressources.

Pour saisir un nouveau code d'activation, nous vous recommandons d'utiliser le plug-in MDR pour Kaspersky Security Center.

Pour saisir un nouveau code d'activation pour Kaspersky Managed Detection and Response dans Kaspersky Security Center avec plug-in MDR, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Licences**.
2. Cliquez sur le bouton **Activer la solution** et saisissez le code d'activation dans le panneau qui s'affiche.
3. Sélectionnez les locataires auxquels les utilisateurs de ce Serveur d'administration auront accès.

Le nouveau code d'activation est appliqué. Kaspersky Managed Detection and Response fonctionne sous la licence fournie.

Pour remplacer le code d'activation actuel par un nouveau dans la Console MDR en ligne, procédez comme suit :

1. Cliquez sur l'onglet **Licensing**.
2. Cliquez sur le lien **Enter a new activation code**.
3. Saisissez un nouveau code d'activation et cliquez sur **Continue**.
4. Sélectionnez votre région et cliquez sur **Confirm and activate**.

Gestion des licences dans Kaspersky Security Center

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Si votre organisation dispose de plusieurs licences en cours de validité, vous ne pouvez les gérer que dans Kaspersky Security Center.

Le rôle **Administrateur MDR** est requis pour la gestion des licences.

Pour afficher les licences :

Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Licences**.

La liste **Licences de votre organisation** s'affiche. Le panneau supérieur présente des informations générales sur les licences :

- Région
- [Niveau de la licence commerciale](#)
- Nombre total et limite des ressources connectées

L'onglet **Active** affiche uniquement les licences actuelles. Cliquez sur l'onglet **Toutes** pour afficher toutes les licences de votre organisation.

Le tableau présente les informations suivantes sur les licences :

Nom de la licence

Nom de la licence qui comprend différentes informations comme le niveau de licence et le nombre maximal de ressources.

Ressources connectées/Limite

Le nombre de ressources qui utilisent cette licence et la limite.

La limite du nombre maximal de ressources de la licence est mise en évidence en rouge lorsqu'elle est dépassée.

Ce nombre n'inclut pas les hôtes avec des fichiers de configuration BLOB créés avant le 1er janvier 2024. Pour résoudre ce problème, effectuez une mise à jour du fichier BLOB dans les paramètres du locataire et appliquez-le aux ressources du locataire. Reportez-vous à la rubrique suivante pour plus de détails : [À propos du fichier de configuration MDR](#).

Identifiant

L'identifiant de la licence.

Date d'expiration

La date de fin de la durée de validité de la licence est mise en évidence en rouge si la licence est expirée ou expire dans 14 jours ou plus tôt.

État

L'un des statuts suivants :

- Active
- Expirée
- Refusée
- Non utilisée
- Remplacée

Nom du client

Masqué par défaut. Vous pouvez activer cette colonne dans le menu du tableau.

Pour télécharger un fichier CSV qui affiche les licences par locataire (plug-in MDR version 2.4.2),

Sous l'onglet **Active**, cliquez sur **Exporter par locataires au format CSV**.

Le fichier CSV comprend la répartition des ressources par locataire pour chaque licence.

Pour afficher les licences par locataires (plug-in MDR version 2.5.0 ou ultérieure),

Sous l'onglet **Active**, cliquez sur **Afficher l'utilisation des licences par locataire**.

Le tableau affiche la répartition des ressources par locataire pour chaque licence.

Pour télécharger le [fichier de configuration MDR](#) pour une licence :

Sélectionnez la colonne **Archives pour la configuration des ressources** et cliquez sur **Download**.

Pour saisir un nouveau code d'activation,

Cliquez sur le bouton **Enter a new activation code** et saisissez le code d'activation dans le panneau qui s'affiche.

Le [niveau de licence](#) et la région de la nouvelle licence doivent correspondre au niveau de licence et à la région des autres codes d'activation de votre organisation.

Pour supprimer un code d'activation :

1. Sélectionnez le bouton radio situé à côté du code d'activation que vous souhaitez supprimer, puis cliquez sur l'icône .
2. Dans la fenêtre qui s'ouvre, confirmez la suppression du code d'activation.
L'état de la licence devient alors **Not used**. Vous pouvez saisir de nouveau le code d'activation supprimé.

Résolution des problèmes de licence

Si vous avez activé la solution MDR sur vos ressources et si la section **Licence** de la Console MDR en ligne affiche moins de ressources qu'il n'y en a de connectées à la solution MDR, reportez-vous à la liste suivante des causes possibles et leurs solutions respectives.

La solution MDR est activée sous plusieurs licences

Solution :

Activez toutes les clés de licence dans le plug-in MDR. La Console MDR en ligne ne prend pas en charge l'activation de plusieurs clés de licence MDR.

La solution MDR a été activée sur les ressources avant le 01/01/2024 à l'aide du Fichier de configuration MDR (BLOB)

Solution 1 :

1. [Télécharger un nouveau fichier de configuration MDR \(BLOB\)](#).
2. Appliquer le nouveau fichier de configuration MDR (BLOB) sur vos ressources.

Solution 2 :

[Appliquer un code d'activation](#)  pour activer la solution MDR sur vos ressources.

Certaines de vos ressources utilisent Kaspersky Endpoint Security for Windows version 12.9 ou antérieure, et la solution MDR pour ces ressources est activée à l'aide d'un fichier clé.

Solution :

[Appliquer un code d'activation](#)  pour activer la solution MDR sur vos ressources. L'activation à l'aide d'un fichier clé sur de telles ressources est prise en charge de manière limitée et n'est pas recommandée.

Vous avez utilisé un fichier clé pour la licence Kaspersky Next Complete Security, Kaspersky Optimum Security, Kaspersky Next MXDR Optimum ou Kaspersky Symphony MDR afin d'activer Kaspersky Endpoint Security for Windows version 12.9 ou une version antérieure.

Solution :

[Appliquer un code d'activation](#) pour activer la solution MDR sur vos ressources.

À propos de l'Accord MDR

L'Accord MDR constitue un accord contraignant entre vous et AO Kaspersky Lab, stipulant les conditions d'utilisation de la solution.

Lisez attentivement l'Accord MDR avant de commencer à utiliser la solution.

Vous pouvez afficher l'Accord MDR :

- Lors de l'activation de Kaspersky Managed Detection and Response.
- En cliquant sur le lien **Conditions d'utilisation de la solution MDR** dans le groupe **Conditions d'utilisation de la solution MDR** : section **MDR** de Kaspersky Security Center → **Utilisation de MDR** → **Conditions d'utilisation de la solution MDR**.

Vous acceptez les termes de l'Accord MDR en confirmant que vous acceptez l'Accord MDR lors de l'activation de la solution. Si vous n'acceptez pas l'Accord MDR, annulez l'activation de Kaspersky Managed Detection and Response et n'utilisez pas la solution.

Collecte des données

Pour que certains composants de Kaspersky Managed Detection and Response fonctionnent, il est nécessaire que Kaspersky traite les données de l'utilisateur. Les composants n'envoient pas de données sans l'autorisation de l'administrateur de Kaspersky Managed Detection and Response.

La liste des données utilisateur dépend de la région dans laquelle la solution est utilisée. Pour votre région, la liste des données utilisateur peut différer de celle figurant dans cette section.

Kaspersky protège toute information reçue conformément à la loi et aux règles applicables de Kaspersky. Les données sont transmises par un canal sécurisé.

Liste des données sur les événements se produisant sur les ressources de l'Utilisateur

Afin de détecter les menaces nouvelles et complexes pour la sécurité des données et leurs sources, ainsi que les menaces d'intrusion, et de prendre des mesures rapides pour augmenter la protection des données stockées et traitées avec un ordinateur par le Client, celui-ci s'engage à fournir automatiquement les informations suivantes pour recevoir le Service :

- Date de l'installation et de l'activation du logiciel, nom complet et version du logiciel, y compris des informations sur les mises à jour installées et la localisation linguistique du logiciel.
- Informations sur le logiciel installé sur l'ordinateur : version du système d'exploitation, date du téléchargement et mises à jour installées, objets de noyau, pilotes, services, entrées Autostart, programmes automatiquement lancés lors de différents événements du système (par exemple le démarrage du système d'exploitation, la connexion de l'utilisateur, etc.) et leurs configurations, extensions de navigateurs, extensions de Microsoft Internet Explorer, extensions de système d'impression, extensions de Windows Explorer, extensions « shell » de système d'exploitation, sommes de contrôle d'objet chargé (MD5), éléments Active Setup, applications de panel de contrôle, versions du navigateur et de la messagerie du client.
- Informations sur les autorisations du système de fichiers, bit effectif pour les autorisations du système de fichiers, versions des autorisations du système de fichiers, variables d'environnement et noms des appels système.
- Informations sur les autorisations héritées pour un fichier système.
- Informations sur le nom de l'ordinateur, adresses IP, passerelles par défaut, adresses et matériel MAC, y compris une somme de contrôle du numéro de série de HDD, 12 derniers octets de l'ID de sécurité de l'ordinateur (SID) et identifiant de zone de sécurité extrait du flux de données NTFS, attributs d'Active Directory du compte de l'ordinateur, y compris le contenu de msDS-AllowedToActOnBehalfOfOtherIdentity, dNSHostName, distinguishedName, sAMAccountName, userAccountControl.
- Informations sur les outils logiciels utilisés afin de résoudre les problèmes du logiciel installé sur l'ordinateur de l'Utilisateur, ou afin de changer ses fonctionnalités, et codes de retour reçus après l'installation de chaque élément du logiciel.

- Informations sur l'état de la protection antivirus de l'ordinateur, y compris les versions et les dates et heures de publication des bases antivirus utilisées, statistiques sur les mises à jour et les connexions aux services Kaspersky Lab, identifiants des tâches, identifiants et versions des composants logiciels effectuant l'analyse, indicateurs de l'environnement de test interne de Kaspersky, codes d'erreur primaires pour un événement spécifique, codes d'erreur secondaires pour un événement spécifique et numéros ordinaux des événements.
- Clé de licence et numéro de série des produits Kaspersky Lab, noms et versions de ces produits. Identifiants des installations de produits Kaspersky Lab et description client du fichier d'information de la licence.
- Informations sur les comptes utilisateur du Client : nom du compte utilisateur, nom de l'utilisateur, identifiant du système d'exploitation, informations de connexion, privilèges, adhésions à des groupes, types de session de connexion au système, nom du paquet d'authentification, noms de domaine, noms DNS utilisés pour l'authentification des sessions de connexion au système, nom du serveur utilisé pour l'authentification, nom du principal utilisateur (UPN) du compte, du SID, des attributs d'Active Directory du compte, y compris e-mail, altSecurityIdentities, sAMAccountName.
- Intégralité du contenu des journaux du système d'exploitation.
- Informations sur les systèmes d'appel.
- Informations sur la détection des programmes de Kaspersky Lab prenant en charge Kaspersky Managed Detection and Response.
- Informations sur les e-mails reçus, par exemple adresses électroniques de l'expéditeur et du destinataire, objet, et informations sur les pièces jointes, par exemple nom du fichier joint, taille, hash (MD5), résultats d'analyse du format de fichier.
- Informations sur les coordonnées de la zone de l'écran où la capture d'écran a été réalisée.
- Informations sur les connexions au réseau : ports et adresses IP expéditeurs et destinataires, indices de zone IPv6, direction de la connexion au réseau (entrante/sortante), types et masques des requêtes DNS réalisées, codes d'erreur pour une opération de requête DNS, réponse à une requête DNS, serveur DNS demandé.
- Données et méthodes de connexion HTTP, y compris les adresses web visitées, les URL de référence, les agents utilisateurs, les informations sur la poignée de main TLS : version du protocole TLS, nom crypté du serveur à partir de l'extension SNI, hachage MD5 et SHA1 du certificat, nom commun du sujet principal et liste des noms DNS des sujets supplémentaires, nom de l'autorité de certification, numéro de série du certificat délivré par l'autorité de certification, résultat de la vérification du certificat, suite de chiffrement utilisée, période de validation du certificat, valeurs décimales JA3 des paquets hello du client et du serveur et leurs hachages MD5, et données du protocole d'authentification du réseau : le hachage MD5 des données pour l'authentification Kerberos, le nom du compte ou de l'ordinateur, le nom du domaine Kerberos auquel appartient le nom du serveur, le domaine auquel appartient le nom du client, l'UPN du compte, le paquet cryptographique utilisé pour le ticket Kerberos émis, le masque de drapeau du ticket Kerberos au format hexadécimal, l'heure d'émission du ticket Kerberos, l'heure d'expiration du ticket Kerberos, la date d'expiration du ticket (après laquelle le ticket ne peut plus être renouvelé) et le nom du contrôleur de domaine utilisé pour émettre le ticket Kerberos.
- Informations sur les protocoles des couches d'application : taille de la requête de recherche LDAP, filtre de la requête de recherche LDAP, nom unique de la requête de recherche LDAP, liste des attributs de la requête de recherche LDAP.
- Informations .NET : nom complet de la version .NET téléchargée, indicateurs d'assemblage pour la version .NET téléchargée, indicateurs de module pour le module .NET téléchargé, nom de domaine pour la version .NET téléchargée, modules pour le stub MSIL généré, informations sur la méthode gérée : espace de nommage de la méthode gérée d'interopération, nom de la méthode gérée d'interopération, signature de la méthode gérée d'interopération, signature de la méthode native et signature du stub de la méthode.

- Informations concernant les fichiers traitées dans le système d'exploitation : nom et chemin du fichier, taille, attributs, types de fichier et d'objet, résultats de l'analyse du format du fichier, somme de contrôle (MD5), adresse Internet à partir de laquelle le fichier a été téléchargé, adresse email de l'expéditeur ayant envoyé le fichier et l'objet de l'email, le contenu du fichier système de la structure VERSIONINFO à partir des métadonnées du fichier, informations sur l'éditeur si le fichier a été signé, ID utilisateur du propriétaire du fichier, ID du groupe de propriétaires du fichier, horodatage du dernier accès au fichier, horodatage de la dernière modification des métadonnées du fichier, création du fichier, masques de l'indicateur de la signature numérique, horodateurs et codes des opérations sur les fichiers et objets, nombre de lancements de fichiers exécutables, identifiant du format de fichier, chemin complet de l'objet et chemin du conteneur de l'objet, contenus du fichier d'exécution automatique (autorun), le nom du fichier et le chemin menant au fichier sur la ressource réseau distante accédée.
- Contenu du répertoire \etc\.
- Données de sortie de commande.
- Données auditd : résultat de l'opération, description de l'opération, type d'événement, utilisation de l'opération.
- Informations sur le processus : identifiant du processus (PID), suivi des appels de processus, informations sur le fichier exécutable du processus et sa ligne de commande, informations sur le processus parent, hash MD5 du code d'erreur de calcul du fichier exécutable, codes d'erreur primaires, informations sur l'intégrité du processus, informations de connexion à la session, ligne de commande, arguments de ligne de commande pour le processus, variables d'environnement pour le processus cible, identifiant unique du journal d'activité du processus, nom et/ou adresse du site d'injection de code, informations sur les droits d'accès pour le processus, codes d'erreur pour le calcul du hash MD5 d'un objet à partir de la ligne de commande du processus, liste des enveloppeurs de l'objet, répertoire de travail initial pour le processus cible, tableau d'identifiants (PID) pour les processus complets.
- Informations sur le registre : noms, sections et valeurs.
- Informations sur les opérations distantes : le nom de l'ordinateur distant et nom complet (« fully qualified name » ou FQDN) de l'ordinateur distant sur lequel l'opération distante a été réalisée, nom du compte utilisateur à l'origine de l'opération distante, identifiant système du processus distant à l'origine de l'opération distante, heure de début du processus distant à l'origine de l'opération distante, nom de l'espace de nommage de l'utilisateur des événements WMI, nom du filtre des événements WMI de l'utilisateur, nom de l'utilisateur créé des événements WMI et code source de l'utilisateur des événements WMI.
- Informations sur les erreurs : code d'erreur du calcul MD5, code d'erreur d'accès aux fichiers, codes d'erreur primaires et codes d'erreur secondaires.

- Informations sur les tâches de réponse aux événements créées par les spécialistes de Kaspersky Lab et de l'Utilisateur : nom et type de l'événement, date et heure auxquelles l'événement s'est produit, paramètres et résultats de la tâche de réponse (informations sur l'objet [chemin d'accès à l'objet, nom et taille de l'objet, sommes de contrôle MD5 et SHA256], informations sur la mise en quarantaine de l'objet, informations sur la suppression de l'objet, informations sur l'arrêt du processus, informations sur la suppression d'une clé/branche de registre, informations sur le démarrage du processus, informations sur les objets demandés par les spécialistes de Kaspersky Lab pour une analyse détaillée avec le consentement de l'Utilisateur [nom, chemin, taille et type de l'objet, sommes de contrôle MD5 et SHA256, description de l'objet, date et heure du traitement de la demande de fichier, contenu du fichier], informations sur l'installation et la suppression de l'isolation réseau de l'appareil, informations sur les erreurs résultant de la tâche de réponse), résultat de la tâche d'analyse IOC : adresse IP et adresse physique issues de la table ARP, nom et type de l'enregistrement de ressource DNS, adresse IP, historique et informations sur le navigateur, ID et nom d'enregistrement de la source de données dans le journal d'événements, nom du journal d'événements, nom d'utilisateur, heure de l'événement, hash, nom complet et taille du fichier, adresse IP distante et port connecté au moment de l'analyse, adresse IP de l'adaptateur local, port ouvert sur l'adaptateur local, protocole sous forme de nombre, nom du processus, arguments du processus, chemin du fichier du processus, PID Windows du processus et du processus parent, date et heure de démarrage du processus, nom et description du service, chemin et nom de la DLL du service (pour svchost), chemin et nom du fichier exécutable du service, PID Windows, type, statut et mode de démarrage du service, nom, lettre et type de volume, valeur du registre Windows, valeur de la ruche du registre, chemin de la clé de registre, paramètre du registre, adresse physique de l'appareil, nom et version du système d'exploitation, nom réseau de l'appareil, domaine ou groupe de travail.
- Données sur les scripts en cours d'exécution sur l'ordinateur : arguments de ligne de commande, contenu du script ou d'une partie du script en cours d'exécution sur l'ordinateur, contenu de l'objet ou d'une partie de l'objet reçu par AMSI.
- Données sur les commandes reçues par l'application console, y compris les interpréteurs de ligne de commande, utilisant la redirection d'entrée via un canal ou un fichier, ainsi que les commandes exécutées par l'utilisateur dans les applications console, y compris les interpréteurs de ligne de commande.

Si la solution MDR s'intègre à Kaspersky Endpoint Detection and Response Expert, les données supplémentaires sont répertoriées ci-dessous :

- Informations à propos des fichiers analysés :
 - somme de contrôle (MD5) de l'objet en cours de traitement ; somme de contrôle (SHA256) de l'objet en cours de traitement ; nom de l'objet en cours de traitement ; taille de l'objet en cours de traitement ; date et heure de création d'un objet en cours de traitement ; indicateur montrant que la signature numérique du module chargé est présente et valide ; informations relatives à l'auteur de la signature du fichier en cours de traitement ; indicateur de confiance de l'objet traité d'après KSN ; format de l'objet en cours de traitement ; informations relatives aux résultats de la vérification de la signature des fichiers ; indicateur de confiance du module dont l'intégrité est vérifiée par le Logiciel.
- Informations à propos des alertes et des technologies de détection :
 - date et heure de publication des bases de données du Logiciel ; verdict du Logiciel sur l'objet en cours de traitement ; indicateur de détection de débogage ; identifiant de la signature déclenchée dans les bases de données antivirus du Logiciel ; classe du danger de la vulnérabilité ; détecter l'identifiant généré par le Logiciel pour l'utilisateur ; nom de l'application malveillante ou du logiciel légitime détecté qui peuvent être utilisés pour endommager l'appareil ou les données de l'utilisateur ; identifiant de l'image du système d'exploitation invité Kaspersky Sandbox ; données du journal interne généré par le module antivirus du Logiciel pour un objet en cours de traitement ; hachage MD5 de l'adresse IP du nœud Kaspersky Sandbox ; numéro d'ordre d'un objet en train d'être de nouveau analysé ; l'identifiant d'enregistrement de la base de données du Logiciel ; valeur du niveau de l'application malveillante détectée ou du logiciel légitime détecté qui peuvent être utilisés pour endommager l'ordinateur ou les données de l'utilisateur ; état de fonctionnement du composant du Logiciel ; date et heure de la détection.

- Informations à propos des résultats de la vérification des données de télémétrie après le déclenchement d'une règle d'indicateur d'attaque (IOA) :

- capacités attribuées à un objet en cours de traitement (pour les systèmes d'exploitation basés sur Unix) ; Informations relatives aux événements des journaux système : heure de l'événement, nom du journal dans lequel l'événement a été détecté, type et catégorie de l'événement, nom de la source de l'événement et description de l'événement ; identifiant de l'événement enregistré dans le journal des événements Windows ; horodatage des bases de données du Logiciel ; taille de l'objet en cours de traitement ; informations sur le groupe d'utilisateurs ; date et heure de création d'un objet en cours de traitement ; nom de l'objet en cours de traitement ; somme de contrôle (MD5) de l'objet en cours de traitement ; masque binaire des paramètres de l'objet en cours de traitement ; identifiant de la signature déclenchée dans les bases de données antivirus du Logiciel ; identifiant unique de la session de connexion ; indicateur montrant que la signature numérique de l'objet en cours de traitement est présente et valide ; attributs du processus ayant attaqué le Logiciel Autodéfense ; paramètres actuels du Logiciel ; nom du fournisseur du Logiciel ; nom du Logiciel ; identifiant de l'appareil qui a établi la connexion à distance avec le système ; chemin d'accès vers l'objet en cours de traitement ; valeur de l'élément de registre Windows ; type de l'objet détecté par le Logiciel ; identifiant du compte à partir duquel le processus contrôlé a été lancé ; identifiant de processus système (PID) ; type de contrôleur pour le périphérique USB ; type de fonction du système rappelé pour exécuter un nouveau processus (pour les systèmes d'exploitation basés sur Unix) ; type de lancement du service Windows ; somme de contrôle (SHA256) de l'objet en cours de traitement ; date et heure de la dernière modification de l'objet en cours de traitement ; adresse Internet en cours de traitement ; adresse email de l'expéditeur ou parties de l'adresse email en cours de traitement ; code d'opération de fichier ; nom de l'appareil de l'utilisateur ; attributs du fichier exécutable en cours de traitement ; version du système d'exploitation, numéro de version du système d'exploitation, numéro de mise à jour du système d'exploitation, édition du système d'exploitation, informations détaillées relatives à l'édition du système d'exploitation ; famille du système d'exploitation ; ligne de commande ; informations relatives à l'auteur de la signature du fichier en cours de traitement ; méthode de requête http ; verdict du Logiciel sur l'objet en cours de traitement ; arguments de la ligne de commande pour le processus ; adresses IP ou sommes de contrôle des adresses IP de la source et de la destination de la connexion réseau en cours de traitement ; nom de la technique d'attaque MITRE ; date et heure de publication des bases de données du Logiciel ; format de l'objet en cours de traitement ; description d'un objet en cours de traitement comme défini dans les propriétés de l'objet ; Source HTTP ; nom et version du SE ; date et heure de la signature du fichier ; réponse du serveur DNS ; volume du trafic sortant ; type de système de fichiers de volume ; autorisations d'accès à l'objet en cours de traitement ; indicateurs ouverts pour un objet en cours de traitement ; le type de compte utilisateur à partir duquel l'objet potentiellement malveillant a été lancé ; date et heure de réception des données ; somme de contrôle (SHA1) d'un objet en cours de traitement ; résultat de l'action avec l'objet en cours de traitement ; type de session de connexion ; identifiant de zone de sécurité extrait du flux NTFS ; identifiant du message électronique ; opérations des fichiers détectés avec l'objet en cours de traitement ; adresse DNS du service Web auquel l'utilisateur a accès ; nom unique de l'objet ; niveau d'intégrité de l'objet en cours de traitement ; en-tête de la requête http en cours de traitement ; données d'une application tierce ayant causé une erreur : le nom et le chemin d'accès du fichier image de l'application, la taille du fichier image de l'application et la somme de contrôle (MD5, SHA256, SHA-1), l'identifiant de processus de l'application (PID), date et heure de la compilation et de la création du fichier image du processus de l'application, pile mémoire du processus de l'application et adresse mémoire du processus de l'application où une erreur s'est produite, temps d'utilisation de l'application avant que l'erreur ne se produise, noms, versions et sommes de contrôle (MD5, SHA256, SHA-1) des fichiers des composants de l'application ; indicateurs de requête du réseau HTTP/HTTPS : URL de la requête, type de bibliothèque open source, nom de domaine de la requête, fournisseur de CDN, méthode de la requête, heure de début de la requête, taille de paquet de la requête, durée totale de la requête, code de statut, taille de paquet de la réponse, type de contenu de la réponse, heure de début de l'en-tête de la requête, heure de fin de l'en-tête de la requête, heure de début du corps de la requête, heure de fin du corps de la requête, heure de début de l'en-tête de la réponse, heure de fin de l'en-tête de la réponse, heure de début du corps de la réponse, heure de fin du corps de la réponse, nombre de redirections, nombre d'échecs de résolution DNS, nombre total de résolutions DNS, nombre d'hôtes résolus à la fois, résultat d'une résolution unique, heure de début d'une résolution unique, heure de fin d'une résolution unique, indication de réussite éventuelle de la résolution, nombre d'échecs de connexion au socket, nombre total de connexions au socket, adresse de destination d'une connexion unique, heure de début d'une connexion unique, heure de fin d'une connexion unique, heure de début d'un échange d'authentification unique, heure de fin d'un échange d'authentification unique, type de HTTP, version du HTTP, type de SSL, type de suite de chiffrement, indication de réussite éventuelle de la connexion, informations sur l'échec de la connexion, informations sur l'exception de requête et informations sur la pile quand la réponse est anormale ; date et heure d'expiration du certificat ; version complète du Logiciel ; nombre d'objets transférés ; type de disque ; paramètres des tâches du planificateur de tâches du système d'exploitation ; espace disque total et quantité

actuellement utilisée ; numéros de port de la source et de la destination de la connexion réseau en cours de traitement ; valeur de confiance de détection d'applications malveillantes ou de logiciels légitimes qui peuvent être utilisés pour endommager l'ordinateur ou les données de l'utilisateur ; date et heure d'émission du certificat ; identifiant de la technique d'attaque MITRE ; identifiant du service ; nom de la clé de registre Windows ; objet du message électronique en cours de traitement ; date et heure de la fin du processus en cours de traitement ; nom de l'espace de nommage pour le consommateur de l'événement WMI ; heure de l'évènement ; nom du filtre utilisé par le consommateur de l'événement WMI ; le mode de fonctionnement du module de protection du Logiciel ; nom de l'émetteur du certificat ; variables d'environnement attribuées à un objet en cours de traitement (pour les systèmes d'exploitation basés sur Unix) ; type de notification qui a déclenché l'envoi de statistiques ; consommateur de l'événement WMI ; contenu en fragments de l'objet en cours de traitement ; paramètres de la tâche de transfert d'objet ; nom du protocole réseau utilisé dans l'attaque réseau détectée ; version de l'objet en cours de traitement ; nom et chemin d'accès de l'élément de registre Windows ; compteur d'événements ; identifiant de la tâche de transfert d'objet ; masque binaire des options de la requête DNS ; masque binaire des options de la requête DNS ; nom de l'indicateur d'attaque (IOA) ; niveau de gravité de la fenêtre invitant l'utilisateur à interagir ; adresse IP locale ; zone de recherche de requête ; numéro de série raccourci du disque dur ; chaîne de requête ; serveur proxy utilisé ; source de l'objet en cours de traitement ; nom du consommateur de l'événement WMI créé ; numéro de série du certificat ; version de l'indicateur d'attaque (IOA) ; identifiant du mode du contrôleur pour le périphérique USB ; adresse email du destinataire ou parties de l'adresse email en cours de traitement ; identifiant de l'indicateur d'attaque (IOA) ; identifiant du périphérique ; direction d'une connexion réseau ; source du trafic Internet en cours de traitement ; hôte local ou distant ; adresse IP du serveur DNS ; type de la valeur de registre Windows ; identifiant de la tactique d'attaque MITRE ; endroit où le code a été injecté dans le processus ; erreur qui s'est produite lors du traitement de la détection ; hôte auquel une connexion a été établie pour transférer des objets.

- attributs de fichier d'un objet en cours de traitement ; paramètres de sécurité à partir des événements du journal des événements Windows ; raison pour laquelle le fichier a été déplacé dans la catégorie ; le nom du domaine utilisé pour authentifier le propriétaire de la session de connexion ; paramètres des objets Active Directory ; paramètres d'exploitation à partir des événements du journal des événements Windows ; paramètres des sessions utilisateur à partir des événements du journal des événements Windows ; code du type d'objet ; version du composant du Logiciel ; paramètres et propriétés des appareils à carte à puce ; version des statistiques en cours d'envoi ; identifiant de processus système parent (PID) ; adresse IP locale ; paramètres des tâches enregistrés dans les événements du journal des événements Windows ; adresse DNS du service Web auquel l'utilisateur a accès ; adresse Internet en cours de traitement ; paramètres de connexion réseau à partir des événements du journal des événements Windows ; nom de l'application malveillante ou du logiciel légitime détecté qui peuvent être utilisés pour endommager l'appareil ou les données de l'utilisateur ; paramètres des objets Active Directory ; paramètres d'exploitation à partir des événements du journal des événements Windows ; paramètres supplémentaires des événements du journal des événements Windows ; paramètres des sessions utilisateur à partir des événements du journal des événements Windows ; le nom du domaine utilisé pour authentifier le propriétaire de la session de connexion ; identifiant de sécurité du compte utilisateur (SID) ; type d'erreur ; texte du message d'erreur.

Liste des données relatives aux événements détectés à la suite de l'analyse du trafic réseau

Afin de détecter les événements nouveaux et complexes pour la sécurité des données et leurs sources, ainsi que les menaces d'intrusion, et de prendre des mesures rapides pour augmenter la protection des données stockées et traitées avec un ordinateur par le Client, celui-ci s'engage à fournir automatiquement les informations suivantes pour recevoir le Service :

- Informations à propos des fichiers analysés :

somme de contrôle (MD5) de l'objet en cours de traitement ; somme de contrôle (SHA256) de l'objet en cours de traitement ; nom de l'objet en cours de traitement ; taille de l'objet en cours de traitement ; date et heure de création d'un objet en cours de traitement ; indicateur montrant que la signature numérique du module chargé est présente et valide ; informations relatives à l'auteur de la signature du fichier en cours de traitement ; indicateur de confiance de l'objet traité d'après KSN ; format de l'objet en cours de traitement ; informations relatives aux résultats de la vérification de la signature des fichiers ; indicateur de confiance du module dont l'intégrité est vérifiée par le Logiciel.

- Informations à propos des alertes et des technologies de détection :
date et heure de publication des bases de données du Logiciel ; verdict du Logiciel sur l'objet en cours de traitement ; indicateur de détection de débogage ; identifiant de la signature déclenchée dans les bases de données antivirus du Logiciel ; classe du danger de la vulnérabilité ; détecter l'identifiant généré par le Logiciel pour l'utilisateur ; nom de l'application malveillante ou du logiciel légitime détecté qui peuvent être utilisés pour endommager l'appareil ou les données de l'utilisateur ; identifiant de l'image du système d'exploitation invité Kaspersky Sandbox ; données du journal interne généré par le module antivirus du Logiciel pour un objet en cours de traitement ; hachage MD5 de l'adresse IP du nœud Kaspersky Sandbox ; numéro d'ordre d'un objet en train d'être de nouveau analysé ; l'identifiant d'enregistrement de la base de données du Logiciel ; valeur du niveau de l'application malveillante détectée ou du logiciel légitime détecté qui peuvent être utilisés pour endommager l'ordinateur ou les données de l'utilisateur ; état de fonctionnement du composant du Logiciel ; date et heure de la détection.
- Informations à propos de l'origine des objets traités et des connexions réseau :
source de l'objet en cours de traitement ; adresse Internet en cours de traitement ; l'adresse IPv4 du service Web à laquelle l'utilisateur a accédé ; adresse Internet de la source de la requête du service Web (référant) ; hôte ; le nom du domaine utilisé pour authentifier le propriétaire de la session de connexion ; adresse IP locale ; informations relatives au client utilisant un protocole réseau (agent utilisateur) ; adresse email de l'expéditeur ou parties de l'adresse email en cours de traitement ; adresse email du destinataire ou parties de l'adresse email en cours de traitement ; objet du message électronique en cours de traitement ; adresses IP ou sommes de contrôle des adresses IP de la source et de la destination de la connexion réseau en cours de traitement ; numéros de port de la source et de la destination de la connexion réseau en cours de traitement ; nom du protocole réseau utilisé dans l'attaque réseau détectée ; nom du protocole réseau utilisé dans l'attaque réseau détectée.
- Données envoyées à l'assistance technique :
Si un problème est détecté du côté de l'utilisateur qui affecte la qualité de la solution et nécessite l'implication de l'assistance technique, les informations nécessaires, et notamment le nom de l'organisation et l'adresse e-mail de contact, une description du problème et les éléments connexes qui peuvent aider à comprendre et à résoudre le problème seront transmises à l'équipe d'assistance technique. L'adresse e-mail de contact peut être : l'adresse à laquelle la solution est enregistrée, ou l'adresse d'un employé spécifique de l'utilisateur si cet employé a demandé l'aide des experts qui fournissent les solutions.
Le service d'assistance technique crée automatiquement un compte dans les systèmes d'assistance technique, s'il n'y avait pas au préalable de compte associé à l'adresse e-mail transmise par les experts.
La création d'un compte d'employé de l'utilisateur est nécessaire pour assurer la communication entre l'utilisateur et le service d'assistance technique afin de résoudre les problèmes liés à la solution.
Ce compte ne sera utilisé par l'équipe d'Assistance technique que pour résoudre les problèmes liés au Service jusqu'à ce que le propriétaire du compte crée une demande non liée au Service.
- Données envoyées lors de l'envoi de notifications et de rapports d'incident :
L'Utilisateur peut utiliser le Service pour envoyer des notifications dès la survenance d'incidents de sécurité des informations, ainsi que des rapports de synthèse sur les incidents de sécurité des informations, aux destinataires qu'il aura spécifiés.
Lorsque le Service est configuré pour envoyer des notifications et des rapports par courrier électronique, le responsable du traitement traitera les données suivantes : l'identifiant et l'adresse électronique du Destinataire.
Lorsque le Service est configuré pour envoyer des notifications via le bot Telegram, le Responsable du traitement traitera les données suivantes : l'identifiant de l'utilisateur, l'identifiant du destinataire de la notification, une bannière indiquant si le destinataire de la notification est abonné au bot Telegram, un lien vers le chat du destinataire de la notification avec le bot Telegram.

Collecte de données lors de l'utilisation de Kaspersky Endpoint Agent

Pour plus d'informations sur la collecte de données lors de l'utilisation de Kaspersky Endpoint Agent, reportez-vous à la section [Kaspersky Endpoint Agent pour Windows](#).

Régions de traitement des données

Le tableau ci-dessous répertorie les régions dans lesquelles les données utilisateur sont traitées conformément à l'Accord relatif au traitement des données de Kaspersky Managed Detection and Response.

Régions de traitement des données

Région d'utilisation de la licence	Région du traitement des données
Europe, Canada	Europe
Royaume d'Arabie saoudite	Royaume d'Arabie saoudite
Russie et autres régions, sauf celles répertoriées ci-dessus	Russie

La région de traitement des données dépend de la région que vous sélectionnez lors de l'[activation](#) de Kaspersky Managed Detection and Response afin de garantir la conformité aux réglementations en matière de traitement des données des utilisateurs.

À propos de l'Accord sur le traitement des données

L'*Accord de traitement des données* (DPA) fait partie intégrante du Contrat de Kaspersky Managed Detection and Response. L'Accord de traitement des données concerne le traitement des données utilisateur par AO Kaspersky Lab au nom d'un utilisateur.

Le contenu de l'*Accord de traitement des données* (DPA), sa disponibilité dans les interfaces de la solution et la liste des données de l'utilisateur dépendent de la région d'utilisation de la solution.

Vous pouvez afficher l'Accord de traitement des données :

- Lors de l'activation de Kaspersky Managed Detection and Response (pour certaines régions uniquement).
- Dans la section **À propos** de la Console MDR en ligne : <https://mdr.kaspersky.com/about> (pour certaines régions uniquement).

La section **À propos** n'est disponible que pour les utilisateurs connectés.

- Dans l'ensemble des documents reçus au moment de l'achat de la solution Kaspersky Managed Detection and Response (pour certaines régions uniquement).

Lisez attentivement l'Accord de traitement des données avant de commencer à utiliser la solution.

Vous confirmez avoir lu et compris l'intégralité de l'Accord de traitement des données lorsque vous activez la solution ou lorsque vous achetez la solution Kaspersky Managed Detection and Response. Si vous n'acceptez pas que vos données soient traitées conformément aux Conditions de traitement des données, annulez l'activation de Kaspersky Managed Detection and Response et n'utilisez pas la solution.

Interfaces de Kaspersky Managed Detection and Response

Cette section fournit des informations sur les interfaces utilisateurs de Kaspersky Managed Detection and Response.

Vous pouvez utiliser Kaspersky Managed Detection and Response en utilisant les interfaces suivantes :

- Portail Kaspersky Managed Detection and Response (ci-après également appelée Console MDR en ligne).

La Console MDR en ligne est disponible à l'adresse <https://mdr.kaspersky.com/> une fois que vous vous êtes connecté. Pour vous connecter, utilisez l'adresse e-mail et le mot de passe du compte du [site Internet de Kaspersky créé lors de l'activation](#) de Kaspersky Managed Detection and Response.

- Section **MDR** dans [Kaspersky Security Center Web Console](#) ou dans Kaspersky Next Expert View.

Afin d'utiliser Kaspersky Security Center Web Console avec Kaspersky Managed Detection and Response, vous devez [télécharger et configurer](#) le plug-in MDR dans Kaspersky Security Center Web Console. Dans Kaspersky Next Expert View, le plug-in MDR est préinstallé.

Pour accéder aux fonctions de Kaspersky Managed Detection and Response, dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, cliquez sur **Surveillance et rapports** → **MDR**.

Les capacités et les fonctions disponibles dans ces interfaces sont fondamentalement les mêmes, mais nous vous recommandons d'effectuer certaines tâches dans l'une des interfaces, car elle met à disposition un plus grand ensemble de fonctions ou de données. L'interface recommandée est indiquée dans la description des tâches et des scénarios d'utilisation.

L'interface de Kaspersky Security Center est principalement conçue pour accomplir les tâches suivantes :

- [Activation de la solution Kaspersky Managed Detection and Response](#)
- Vérification de l'état des ressources

L'interface de la Console MDR en ligne est principalement conçue pour accomplir les tâches suivantes :

- Tâches du responsable de la sécurité : gestion des incidents
- Tâches de l'administrateur : administration des utilisateurs MDR
- Consultation et gestion des ressources

Section MDR dans Kaspersky Security Center

Vous pouvez utiliser Kaspersky Managed Detection and Response via la section **MDR** de [Kaspersky Security Center Web Console](#) ou de Kaspersky Next Expert View. Pour accéder aux fonctions de Kaspersky Managed Detection and Response, dans Kaspersky Security Center, cliquez sur **Surveillance et rapports** → **MDR**.

La section **MDR** de l'interface Web de [Kaspersky Security Center](#) ² contient les onglets suivants :

- **Incidents.** Contient le lien vers la Web Console de MDR où vous pouvez gérer vos incidents.
- **Paramètres.** Permet d'activer les notifications détaillées et de modifier de langue pour les données d'incident, les notifications et les rapports.
- **Licences.** Permet d'administrer les licences MDR.
- **API.** Contient la liste des connexions API et les fonctions permettant de les gérer.
- **Locataires.** Contient la liste des locataires et les fonctions pour les gérer.
- **États des ressources MDR.** Contient les listes des ressources défectueuses et de toutes les ressources vues.
- **Premiers pas** (Getting Started). Contient les instructions de configuration de la solution MDR.
- **Utilisation de MDR.** Contient les informations sur l'état d'activation de la solution, la licence, la région de stockage de la télémétrie, le fichier de configuration KPSN et l'état d'acceptation des Conditions d'utilisation.

Vous pouvez aussi [ajouter](#) ² le widget **Ressources MDR par état** dans le volet **Surveillance et rapports** → **Tableau de bord** de bord de Kaspersky Security Center.

Configuration du plug-in MDR dans Kaspersky Security Center

Cette section contient des informations sur la configuration initiale du plug-in MDR dans Kaspersky Security Center pour l'utilisation de Kaspersky Managed Detection and Response.

Configuration des droits d'accès dans Kaspersky Security Center

Vous devez définir des droits d'accès pour chaque utilisateur de Kaspersky Security Center Web Console ou de Kaspersky Next Expert View qui utilisera les fonctions MDR de Kaspersky Security Center. Les droits d'accès dépendent des actions que vous souhaitez que les utilisateurs puissent effectuer.

Vous pouvez créer automatiquement les rôles MDR avec des droits d'accès prédéfinis en cliquant sur le lien dans la première étape de l'onglet **Premiers pas** (Getting Started) de la section **MDR** de Kaspersky Security Center.

Pour définir les droits d'accès, procédez comme suit :

1. Dans Kaspersky Security Center, accédez à la section **Utilisateurs et rôles** → **Rôles**, puis créez un nouveau rôle. Pour savoir comment créer des rôles, consultez l'aide [Kaspersky Security Center Windows](#) ², l'[aide de Kaspersky Security Center Linux](#) ² ou l'[aide de Kaspersky Next Expert View](#) ².
2. Dans l'onglet **Privilèges d'accès** d'un nouveau rôle, définissez le droit d'accès **Autoriser** pour les domaines fonctionnels :
 - **Serveur d'administration de Kaspersky Security Center** → **Fonctions générales** → **Intégration de l'application**

Serveur d'administration de Kaspersky Security Center → Fonctions générales → Fonctionnalité de base

Serveur d'administration de Kaspersky Security Center → Fonctions générales → Accéder aux objets quel que soit leur ACL

Ces droits d'accès permettent aux utilisateurs d'activer, de configurer et d'utiliser Kaspersky Managed Detection and Response, ainsi que de mettre fin à son utilisation

- **Kaspersky Managed Detection and Response → Accès aux incidents**

Il est nécessaire de définir le droit d'accès **Autoriser** pour le domaine fonctionnel **Accès aux incidents** pour que les utilisateurs aient accès à la section **MDR** de Kaspersky Security Center. Si le domaine fonctionnel **Accès aux incidents** dispose du droit d'accès **Interdire**, les utilisateurs ne peuvent voir que l'onglet **Premiers pas** de la section **MDR** de Kaspersky Security Center.

- **Kaspersky Managed Detection and Response → Gestion des locataires**

Permet aux utilisateurs de créer, d'afficher et de modifier des locataires.

- **Kaspersky Managed Detection and Response → Accès à l'API REST**

Permet aux utilisateurs d'administrer Kaspersky Managed Detection and Response via l'API REST.

3. Attribuez le rôle créé à tous les utilisateurs qui utiliseront les fonctions MDR de Kaspersky Security Center.

Le tableau suivant montre l'ensemble minimum de droits d'accès.

Ensemble minimal de droits d'accès

Domaine fonctionnel	Autoriser	Refuser
Intégration d'applications	—	✓
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	—	✓
Gestion des réponses	—	✓
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

Les droits d'accès sont définis.

Consultation et modification des paramètres MDR dans Kaspersky Security Center

Vous pouvez consulter et modifier les paramètres du plug-in MDR installé dans Kaspersky Security Center.

Pour afficher et modifier les paramètres, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Paramètres**.
2. Si vous souhaitez recevoir des [notifications détaillées](#) par e-mail, activez l'option **Activer l'envoi des notifications détaillées par email** et cochez la case pour confirmer que vous avez lu et compris les conditions d'envoi des notifications détaillées.
3. Vous pouvez utiliser le paramètre **Langue** afin de sélectionner l'anglais ou le russe pour l'affichage des rapports et des notifications.

4. Cliquez sur le bouton **Enregistrer** dans la partie inférieure de la fenêtre pour enregistrer les paramètres.
Le bouton **Enregistrer** ne devient actif que si vous avez modifié les paramètres.

Utilisation des fonctions du plug-in MDR sur un Serveur d'Administration virtuel

Pour utiliser les fonctions MDR de Kaspersky Security Center sur le Serveur d'Administration virtuel, procédez comme suit :

- Si vous utilisez Kaspersky Security Center pour Windows :
 1. Téléchargez le [fichier de configuration MDR](#) dans Kaspersky Security Center Web Console ou dans la [Console MDR en ligne](#).
 2. Dans Kaspersky Security Center Web Console, sélectionnez le Serveur d'Administration principal (physique) dans lequel se trouve votre Serveur d'administration virtuel.
 3. Activez le commutateur [Kaspersky Private Security Network](#) dans les propriétés du Serveur d'administration principal (physique).
 4. Cliquez sur le bouton **Sélectionner le fichier avec les paramètres du proxy KSN** et sélectionnez le fichier de configuration MDR que vous avez téléchargé.
- Si vous utilisez Kaspersky Next Expert View :
 1. Activez Kaspersky Managed Detection and Response sur le Serveur d'administration principal (physique).
 2. Sur le Serveur d'administration principal (physique), cliquez sur **Suivi et Rapports** → **MDR**, ouvrez l'onglet **Utilisation de MDR** et assurez-vous que la section **Fichier de configuration KPSN pour l'intégration avec le Serveur d'administration de KSC** contient l'état et la version correspondant au fichier de configuration KPSN. Exemple d'état et de version correspondants :

La version du fichier de configuration KPSN est utilisée pour envoyer les données télémétriques à l'infrastructure de Kaspersky MDR

Si l'état ou la version du fichier ne correspond pas, veuillez [contacter le Support technique](#).

Utilisation des fonctions MDR de Kaspersky Security Center via un serveur proxy

Si un serveur proxy est utilisé au sein du réseau utilisé Kaspersky Security Center, vous devez configurer deux variables d'environnement avec les paramètres du serveur proxy selon le protocoles HTTP et HTTPS pour que les fonctions MDR de Kaspersky Security Center fonctionnent. Ces variables d'environnement doivent être définies sur l'hôte sur lequel Kaspersky Security Center Web Console est installée.

Les variables d'environnement prennent le format suivant :

`HTTP_PROXY=<protocol>://<proxy_user_name>:<proxy_user_password>@<host>:<port>`

où :

- <protocol> correspond au format http ou https.
- <proxy_user_name> est le nom d'utilisateur pour l'autorisation sur le serveur proxy.
- <proxy_user_password> est le mot de passe pour l'autorisation sur le serveur proxy.
- <host>:<port> sont le nom ou l'adresse IP du serveur proxy, et son numéro de port.

Exemple de variables d'environnement :

```
HTTP_PROXY=http://proxy_user_name:proxy_user_password@proxy.domain.com:8080  
HTTPS_PROXY=https://proxy_user_name:proxy_user_password@proxy.domain.com:443
```

Il existe deux manières de définir les variables d'environnement :

- Si vous voulez appliquer les paramètres du proxy à toutes les applications sur l'hôte où Kaspersky Security Center Web Console est installée, ajoutez ces variables d'environnement à l'aide du module **Modifier les variables d'environnement système** du système d'exploitation Windows. Pour en savoir plus sur l'utilisation de ce module, consultez la documentation de la version du système d'exploitation que vous utilisez.
- Si vous voulez appliquer ces paramètres du proxy uniquement à Kaspersky Security Center Web Console, ajoutez ces variables d'environnement dans le fichier.env situé dans le dossier d'installation de Kaspersky Security Center Web Console (par défaut, C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\). Si le fichier.env manque dans le dossier d'installation, créez-le.

Après avoir défini les variables d'environnement, il faut redémarrer l'hôte sur lequel Kaspersky Security Center Web Console est installée pour que les modifications soient appliquées.

Modification des certificats pour l'utilisation des fonctions MDR dans Kaspersky Security Center grâce à un serveur proxy ou un logiciel antivirus

Vous devez redéfinir la chaîne de certificats pour la connexion entre Kaspersky Security Center Web Console dotée du plug-in MDR et l'infrastructure de la solution MDR dans les situations suivantes :

- Le serveur proxy disposant d'une connexion TLS est utilisé dans le réseau au sein duquel Kaspersky Security Center s'exécute.
- Un logiciel antivirus avec chiffrement du trafic TLS est exécuté sur l'hôte sur lequel Kaspersky Security Center Web Console est installée.

Pour redéfinir la chaîne de certificats, procédez comme suit :

1. Enregistrez les certificats nécessaires sous forme de fichiers sur votre ordinateur.
 - Pour enregistrer le fichier de certificat du logiciel de chiffrement du trafic, sur l'hôte sur lequel est installée Kaspersky Security Center Web Console, accédez à <https://mdr-ksc.kaspersky.com/> dans le navigateur Chrome, cliquez sur l'icône en forme de cadenas dans la barre d'adresses, cliquez sur **La connexion est sécurisée**, puis sur **Le certificat est valide**, accédez à l'onglet **Détails** puis cliquez sur le bouton **Exporter**. Pour obtenir les instructions relatives aux autres navigateurs, consultez la documentation correspondante.
 - Pour obtenir le certificat de connexion au serveur proxy, contactez votre administrateur réseau.
2. Ajoutez les certificats enregistrés dans le fichier avec l'extension.PEM (par exemple, KL_Root.pem).

3. Placez le fichier.PEM créé dans le dossier d'installation de Kaspersky Security Center Web Console (par défaut, C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\).
4. Ajoutez la variable d'environnement NODE_EXTRA_CA_CERTS au fichier.env situé dans le dossier d'installation de Kaspersky Security Center Web Console. Si le fichier.env manque dans le dossier d'installation, créez-le.

Exemple de la variable :

```
NODE_EXTRA_CA_CERTS="C:\Program Files\ Kaspersky Lab\ Kaspersky Security Center Web Console\KL_Root.pem"
```

Pour appliquer les modifications apportées après la définition de la variable d'environnement, redémarrez l'hôte sur lequel Kaspersky Security Center Web Console est installé.

Masquer et afficher les fonctionnalités MDR dans Kaspersky Security Center

Par défaut, les éléments d'interface liés à Kaspersky Managed Detection and Response s'affichent dans l'interface de Kaspersky Security Center. Si vous n'utilisez pas Kaspersky Managed Detection and Response, vous pouvez masquer ses fonctionnalités dans l'interface. Plus tard, vous pouvez [modifier les paramètres de l'interface](#) pour afficher à nouveau les éléments cachés.

Pour masquer les fonctionnalités MDR dans Kaspersky Next Expert View, procédez comme suit :

1. Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, passez le pointeur de la souris sur votre nom d'utilisateur situé dans le panneau gauche en bas. Le menu des paramètres d'interface apparaît.
2. Cliquez sur **Options d'interface**.
3. Activez ou désactivez les **Afficher les fonctionnalités MDR**.
4. Cliquez sur le bouton **Enregistrer**.

Kaspersky Security Center enregistre la valeur de cette option uniquement pour votre compte utilisateur. D'autres utilisateurs peuvent définir une valeur différente.

La section **MDR** est masquée ou affichée.

Console MDR en ligne

Vous pouvez Kaspersky Managed Detection and Response dans l'interface [Web Console MDR en ligne](#).

La fenêtre de la Console MDR en ligne contient les éléments suivants :

- Menu principal dans le volet gauche de la fenêtre
- Espace de travail dans le volet droit de la fenêtre

Menu principal

Le menu principal contient les sections suivantes :

- **Monitoring.** Contient des widgets qui fournissent des informations synthétiques sur les incidents ressources, les ressources et les réponses.
- **Incidents.** Contient des informations détaillées sur vos incidents et les outils pour les gérer.
- **Assets :** Contient des informations détaillées sur les ressources et les outils pour les utiliser.
- **Settings.** Contient les onglets pour gérer les comptes utilisateurs, les notifications, les paramètres d'incident, les rapports de synthèse, l'API, les locataires et les paramètres généraux.
- **About.** Contient les informations sur la solution, les liens vers l'accord MDR, l'Accord de traitement des données (DPA), la présente aide en ligne et le site Web du Support technique.

Dans la partie inférieure du volet gauche, le contrôle des **Account settings** vous permet d'accéder à la *page Premiers pas*, de modifier la langue de l'interface, d'accéder à la page de votre profil d'utilisateur et de sortir de la Console MDR en ligne.

Espace de travail

L'espace de travail reprend les informations que vous souhaitez consulter dans la Console MDR en ligne. L'espace de travail contient également les éléments de contrôle que vous pouvez utiliser pour configurer le mode d'affichage des informations.

Changement de la langue de l'interface dans Kaspersky Security Center

L'interface MDR de Kaspersky Security Center est disponible dans les langues suivantes :

- Anglais
- Russe
- Allemand
- Espagnol
- Français
- Italien

Pour modifier la langue de l'interface dans Kaspersky Security Center :

1. Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, dans le menu principal, accédez à **Paramètres** → **Langue**.
2. Sélectionnez une des langues de localisation prises en charge.

La langue est modifiée.

Vous pouvez choisir une autre langue à tout moment.

Changement de langue pour les notifications et les rapports dans Kaspersky Security Center

Dans Kaspersky Security Center, vous pouvez sélectionner l'anglais ou le russe pour afficher les données sur les incidents, les notifications et les rapports.

Pour changer la langue des données d'incident, des notifications et des rapports dans Kaspersky Security Center, procédez comme suit :

1. Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, cliquez sur **MDR** → **Paramètres**.
2. Dans la zone **Langue**, sélectionnez **Russe** ou **Anglais**.
3. Cliquez sur le bouton **Enregistrer**.

La langue est modifiée.

Vous pouvez choisir une autre langue à tout moment.

Le changement de langue ne s'applique qu'aux notifications et rapports à venir. Les notifications et rapports déjà générés resteront dans la langue choisie précédemment.

Changement de langue de l'interface dans la Console MDR en ligne

La Console MDR en ligne est disponible dans les langues suivantes :

- Anglais
- Russe

Pour modifier la langue de l'interface de la Console MDR en ligne, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à la section **Account settings** située dans le panneau inférieur gauche. Cette section contient la zone **Language**.
2. Dans la zone **Language**, cliquez sur la langue que vous souhaitez appliquer à l'interface de la Console MDR.

La langue est modifiée. Vous pouvez choisir une autre langue à tout moment.

À propos du fichier de configuration MDR

Kaspersky Managed Detection and Response utilise un fichier de configuration MDR afin d'activer la solution sur les applications EPP Kaspersky pour les postes de travail (tels que Kaspersky Endpoint Security for Windows) installés sur les [ressources](#).

Le fichier de configuration MDR est généré automatiquement par Kaspersky Managed Detection and Response lorsque vous activez la solution à l'aide d'un code d'activation. Le fichier de configuration MDR est une archive ZIP contenant les fichiers suivants :

- Fichier de configuration [KPSN](#).
- Fichier BLOB (P7) pour le déploiement d'applications EPP prenant en charge l'intégration avec MDR via les politiques de Kaspersky Security Center.

Une fois généré, le fichier BLOB expire dans 5 ans, même si la licence est perpétuelle ou délivrée pour une durée plus longue.

Le fichier BLOB (P7) n'est peut-être pas nécessaire dans les conditions suivantes :

Notez que même si vous n'utilisez pas le fichier de configuration MDR, il est nécessaire d'activer la solution depuis la Console MDR en ligne ou à l'aide du plug-in MDR dans Kaspersky Security Center.

- Vous utilisez uniquement les applications EPP suivantes :
 - Kaspersky Endpoint Security for Windows version – version 12.6 ou ultérieure
 - Kaspersky Endpoint Security for Windows – version 12.8 ou ultérieure en mode Light Agent
 - Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
 - Kaspersky Endpoint Security for Mac version 12.2 ou ultérieure
- Votre organisation utilise uniquement le locataire racine et n'a jamais créé de locataires supplémentaires.
- Vous n'utilisez pas la solution Kaspersky Endpoint Detection and Response Optimum en même temps que la solution Kaspersky MDR. Pour en savoir plus, consultez la section [Activation de la solution MDR dans les applications Kaspersky](#).

Dans ce cas, Kaspersky Endpoint Security pour Windows utilise la licence de Kaspersky Security Center. Si vous utilisez des clients autres que le locataire racine, vous devez télécharger le fichier de configuration MDR pour chaque locataire.

[Téléchargez le fichier de configuration MDR](#) et utilisez-le selon les instructions pour les applications EPP installées sur vos ressources :

- [Kaspersky Endpoint Security for Windows](#)
- [Kaspersky Endpoint Security for Linux](#)
- [Kaspersky Endpoint Security for Mac](#)

À propos de Kaspersky Security Network

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

La solution RDG utilise Kaspersky Security Network (KSN) pour les tâches suivantes :

- Envoi de données télémétriques depuis les ressources.
- Intégration avec le serveur Kaspersky Anti Targeted Attack Platform (EDR).
- Intégration de Kaspersky Endpoint Detection and Response Expert au sein de l'Open Single Management Platform.

Un fichier de configuration KPSN est installé lorsque vous configurez l'intégration avec Kaspersky Anti Targeted Attack Platform (EDR) ou avec Kaspersky Endpoint Detection and Response Expert au sein d'Open Single Management Platform.

Nous vous recommandons de ne pas utiliser de fichier de configuration KPSN pour envoyer les données télémétriques depuis les ressources. Cependant, si votre configuration ne remplit pas les [conditions requises pour un fonctionnement sans fichiers de configuration KPSN](#), vous devez installer un fichier de configuration KPSN sur le Serveur d'administration. Pour plus de détails sur la configuration de KSN, consultez la [documentation de Kaspersky Security Center](#) ². Pour garantir la transmission sécurisée des données télémétriques du client vers Kaspersky Managed Detection and Response, Kaspersky met régulièrement à jour les clés de chiffrement des données de télémétrie MDR. Pour en savoir plus, reportez-vous à l'article suivant : [Mise à jour périodique des fichiers de configuration KPSN](#).

Si vous installez un fichier de configuration KPSN sur le Serveur d'administration de Kaspersky Security Center, KSN est automatiquement désactivé lorsque vous [révoquez votre consentement aux conditions d'utilisation de la solution MDR](#).

Si vous avez ajouté manuellement un fichier de configuration KPSN sur le Serveur d'administration et que vous n'avez pas activé le plug-in MDR pour Kaspersky Security Center, vous devez remplacer ou supprimer manuellement ce fichier de configuration KPSN du Serveur d'administration.

Mise à jour périodique des fichiers de configuration KPSN

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Nous vous recommandons de basculer la solution MDR vers un fonctionnement sans fichiers de configuration KPSN. Pour en savoir plus, reportez-vous à cet article : [Basculement de la solution MDR vers un fonctionnement sans fichiers de configuration KPSN](#). Si vous disposez de ressources qui utilisent des fichiers de configuration KPSN, vous devez mettre à jour les fichiers de configuration KPSN une fois par an. Dans le cas contraire, les données de télémétrie de ces ressources cesseront d'être envoyées à Kaspersky Managed Detection and Response.

Si vous ne pouvez pas pour le moment basculer vers un fonctionnement sans fichiers de configuration KPSN, consultez les informations ci-dessous et suivez les instructions.

Pourquoi la mise à jour des fichiers de configuration est nécessaire

Pour garantir la transmission sécurisée des données télémétriques du client vers Kaspersky Managed Detection and Response, Kaspersky met régulièrement à jour les clés de chiffrement des données de télémétrie MDR. La transmission de la clé publique se fait dans le cadre du fichier de configuration KPSN.

Si vous utilisez le plug-in MDR pour Kaspersky Next Expert View ou Kaspersky Security Center sur site, dans certains cas (veuillez consulter les détails dans le tableau ci-dessous), le fichier de configuration KPSN sera mis à jour automatiquement. Cependant, dans de nombreux cas, vous devez remplacer manuellement le fichier de configuration KPSN installé.

Un mois au plus tard avant l'expiration du fichier de configuration KPSN actuel, Kaspersky vous informera de l'expiration imminente de ce dernier. Il existe deux options de notification :

- Un incident sera créé pour vous informer de l'expiration prochaine du fichier de configuration KPSN actuel.
- Une notification sur l'expiration prochaine du fichier de configuration actuel de KPSN sera publiée dans la Console MDR en ligne. Tout utilisateur se connectant à la Console MDR en ligne verra cette notification.

La solution que vous utilisez pour administrer vos ressources	L'interface utilisée par vos analystes du SOC	Actions requises
Kaspersky Next Expert View	Plug-in MDR installé dans Kaspersky Next Expert View	Connectez-vous à Kaspersky Next Expert View. Lorsque vous vous connectez, le plug-in MDR vous invite à accepter le nouveau contrat KPSN. Le fichier de configuration KPSN sera automatiquement mis à jour une fois que l'Administrateur aura accepté le contrat KPSN. Si le plug-in MDR met à jour le fichier avec succès, vous recevrez une notification concernant la modification du fichier de configuration KPSN. Si le plug-in MDR ne parvient pas à mettre à jour le fichier de configuration KPSN, vous recevrez une notification indiquant la cause du problème : • Votre compte utilisateur ne dispose pas des droits d'accès suffisants pour mettre à jour le fichier. • Une erreur inattendue s'est produite lors de la mise à jour du fichier de configuration KPSN. Si aucune notification ne s'affiche, il est probable que le fichier de configuration KPSN a été mis à jour correctement lors de la connexion d'un autre technicien à Kaspersky Next Expert View. Si vous recevez une notification indiquant que les droits d'accès sont insuffisants pour mettre à jour le fichier de configuration KPSN, contactez votre administrateur Kaspersky Next Expert View (rôle Administrateur principal) pour obtenir de l'aide : Demandez à l'administrateur de se connecter à Kaspersky Next Expert View. Lorsque l'administrateur ouvre une session, le fichier de configuration KPSN est alors mis à jour. Vous pouvez vérifier que le fichier de configuration KPSN est à jour à tout moment. Pour ce faire, dans la section MDR de Kaspersky Security Center, cliquez sur l'onglet Utilisation de MDR. Les informations sur la version actuelle du fichier de configuration KPSN s'affichent. Si une nouvelle version du fichier de configuration KPSN est disponible, vous pouvez utiliser un bouton pour mettre à jour le fichier de configuration KPSN. Si une erreur inattendue se produit lors de la mise à jour, contactez le Support technique Kaspersky.
Kaspersky Next Expert View	Console MDR en ligne OU Vous utilisez l'API pour télécharger les incidents afin de les traiter dans votre propre système	Connectez-vous à Kaspersky Next Expert View. Lancez l'Assistant de configuration initiale pour activer le plug-in MDR. Si votre compte ne dispose pas de droits d'accès suffisants pour activer le plug-in MDR, contactez l'administrateur de votre serveur Kaspersky Next Expert View pour obtenir de l'aide. Suivez ensuite les instructions ci-dessus relatives au serveur Kaspersky Next Expert View et au plug-in MDR. Si une erreur inattendue se produit lors de la mise à jour, contactez le Support technique Kaspersky.
Open Single Management Platform	Plug-in MDR installé dans Open Single Management Platform	Lorsqu'un Administrateur MDR se connecte à Open Single Management Platform, il doit accepter le nouveau contrat KPSN. Le fichier de configuration KPSN est automatiquement mis à jour une fois que l'Administrateur a accepté le contrat KPSN. Si le contrat n'a pas été accepté, les utilisateurs disposant du rôle Administrateur MDR peuvent l'accepter ultérieurement dans la console OSMP. <i>Pour accepter le contrat et mettre à jour le fichier de configuration KPSN :</i> 1. Dans la section MDR de l'interface de la Console OSMP, cliquez sur l'onglet Utilisation de MDR. 2. Développez le bloc Fichier de configuration KPSN pour l'intégration avec le Serveur d'administration de KSC. 3. Activez l'option Accepter le contrat KPSN et cliquez sur Appliquer le fichier de configuration KPSN sur le Serveur d'administration. 4. En outre, si vous avez configuré l'intégration avec Kaspersky Endpoint Detection and Response Expert (sur site), procédez comme suit : a. Développez le groupe fichier de configuration KPSN pour l'intégration avec KEDR Expert. b. Activez l'option Accepter le contrat KPSN et cliquez sur Appliquer le fichier de configuration KPSN pour l'intégration avec KEDR Expert.

La solution que vous utilisez pour administrer vos ressources	L'interface utilisée par vos analystes du SOC	Actions requises
Kaspersky Security Center sur site versions 14 et ultérieures	Plug-in MDR installé dans Kaspersky Security Center en local	Connectez-vous à Kaspersky Security Center. Lors de la connexion, selon la version du plug-in MDR, le fichier de configuration KPSN est mis à jour automatiquement ou après qu'un utilisateur disposant du rôle Administrateur MDR a accepté le nouveau contrat KPSN. Si le plug-in MDR met à jour le fichier avec succès, vous recevrez une notification concernant la modification du fichier de configuration KPSN. Si le plug-in MDR ne parvient pas à mettre à jour le fichier de configuration KPSN, vous recevrez une notification indiquant la cause du problème : • Votre compte utilisateur ne dispose pas des droits d'accès suffisants pour mettre à jour le fichier. • Une erreur inattendue s'est produite lors de la mise à jour du fichier de configuration KPSN. Si aucune notification ne s'affiche, il est probable que le fichier de configuration KPSN a été mis à jour correctement lors de la connexion d'un autre expert à Kaspersky Next Expert View. Si vous recevez une notification indiquant que les droits d'accès sont manquants pour mettre à jour le fichier de configuration KPSN, contactez l'administrateur du serveur d'administration de Kaspersky Security Center pour obtenir de l'aide : Demandez à l'administrateur de se connecter au serveur de Kaspersky Security Center. Lorsque l'administrateur ouvre une session, le fichier de configuration KPSN est alors mis à jour. Si l'administrateur ne reçoit pas la notification concernant la modification du fichier de configuration KPSN, il doit vérifier la version du plug-in MDR installé et, si nécessaire, le mettre à jour vers la version actuelle (plug-in MDR 2.1.17 ou version ultérieure requis). Vous pouvez vérifier que le fichier de configuration KPSN est à jour à tout moment. Pour ce faire, dans la section MDR de Kaspersky Security Center, cliquez sur l'onglet Utilisation de MDR. Les informations sur la version actuelle du fichier de configuration KPSN seront affichées. Si une nouvelle version du fichier de configuration KPSN est disponible, vous pouvez utiliser un bouton pour mettre à jour le fichier de configuration KPSN. Si une erreur inattendue se produit lors de la mise à jour, contactez le Support technique Kaspersky.
Kaspersky Security Center sur site versions 13* ou ultérieures	Console MDR en ligne (le plug-in MDR n'est pas installé dans le Kaspersky Security Center sur site) OU Vous utilisez l'API pour télécharger les incidents afin de les traiter dans votre propre système	Demandez à l'administrateur du de la Console MDR en ligne de : 1. Téléchargez l'archive ZIP MDR à partir de la page Licences. 2. Décompressez le fichier ZIP pour extraire le fichier de configuration KPSN. 3. Envoyer ce fichier à l'administrateur du serveur d'administration de Kaspersky Security Center.
Kaspersky Security Center sur site versions 13* ou antérieures	Plug-in MDR installé dans le Kaspersky Security Center sur site OU Vous utilisez l'API pour télécharger les incidents afin de les traiter dans votre propre système	

Si plusieurs serveurs Kaspersky Security Center sont installés dans votre réseau, vous devez mettre à jour le fichier de configuration KPSN sur chacun d'entre eux.

Mise à jour du fichier de configuration KPSN sur les serveurs KATA

Si votre réseau comporte des serveurs KATA connectés à Kaspersky Managed Detection and Response, vous devez mettre à jour le fichier de configuration MDR sur ces derniers.

La procédure de mise à jour du fichier de configuration MDR dépend de la version de KATA.

Pour mettre à jour le fichier de configuration MDR sur les serveurs KATA versions 8.0 à 8.1 :

1. Connectez-vous à l'interface Web de KATA avec le compte administrateur.
2. Sélectionnez la section **Paramètres**, puis la sous-section **KSN/KPSN et MDR**.
3. Sous **Intégration MDR**, cliquez sur **Se reconnecter**.
4. Dans la fenêtre qui s'ouvre, saisissez les informations d'identification de votre Kaspersky Account.

Une fois les informations d'identification vérifiées avec succès, le fichier de configuration MDR est automatiquement mis à jour sur le serveur.

Pour mettre à jour le fichier de configuration MDR sur les serveurs KATA versions 7.1 et antérieures :

1. Connectez-vous à la console MDR avec le compte Administrateur MDR.
2. Téléchargez l'archive ZIP de configuration MDR depuis la page **Getting Started** :
<https://mdr.kaspersky.com/guide>.
3. Connectez-vous à l'interface Web de KATA avec le compte administrateur.
4. Sélectionnez la section **Paramètres**, puis la sous-section **KSN/KPSN et MDR**.
5. Sous **Intégration MDR**, cliquez sur **Charger** pour charger le fichier de configuration.
La fenêtre de sélection de fichiers s'ouvre.
6. Sélectionnez l'archive téléchargée depuis la Console MDR en ligne et cliquez sur **Ouvrir**.

Le fichier de configuration MDR est mis à jour sur le serveur.

En cas de problème lors de la mise à jour du fichier de configuration MDR, l'administrateur du serveur KATA doit contacter le Support Technique de Kaspersky pour obtenir des instructions sur la mise à jour du fichier de configuration MDR sur le serveur KATA.

Basculement de la solution MDR vers un fonctionnement sans fichiers de configuration KPSN

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

La solution MDR doit utiliser la configuration KPSN dans les scénarios suivants :

- Pour s'assurer que les données de requêtes et de statistiques de KSN ne sont jamais envoyées à une autre région. Sans configuration KPSN, Kaspersky s'assure uniquement que les données sont acheminées vers la région indiquée. Pour en savoir plus, reportez-vous à cet article : [Mise à jour périodique des fichiers de configuration KPSN](#).
- Pour assurer le fonctionnement de la solution MDR lorsqu'une application EPP obsolète est installée sur l'un de vos appareils.

Vous pouvez faire en sorte que la solution MDR fonctionne sans fichiers de configuration KPSN si les conditions suivantes sont remplies :

1. Les versions de l'application EPP qui prennent en charge le fonctionnement sans KPSN sont installées sur toutes vos ressources :
 - Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure
 - Kaspersky Endpoint Security for Windows version 12.6 ou ultérieure dans la configuration de Endpoint Detection and Response Agent
 - Kaspersky Endpoint Security for Windows Light Agent – version 12.8 ou ultérieure
 - Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
 - Kaspersky Endpoint Security for Mac version 12.2 ou ultérieure
 - Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure
 - Kaspersky Embedded Systems Security for Linux – version 4.0 ou ultérieure
 - Kaspersky Industrial CyberSecurity for Nodes Windows 4.5
2. La solution MDR est activée sur toutes vos ressources à l'aide d'un code d'activation ou d'un fichier BLOB qui a été créé au plus tôt le 1er janvier 2024.

Les fichiers BLOB créés à partir du 1er janvier 2024 contiennent des données nécessaires au fonctionnement sans KPSN.

Il est recommandé d'utiliser un code d'activation pour activer la solution MDR pour les applications EPP qui la prennent en charge. Certaines versions des applications EPP ne prennent pas en charge le fonctionnement sans KPSN si vous utilisez un fichier clé pour activer la solution MDR. Pour en savoir plus, consultez l'article suivant : [Configuration matérielle et logicielle requise](#).

Pour faire passer la solution MDR à un fonctionnement sans KPSN :

1. Générez et passez en revue un rapport sur les versions des applications Kaspersky dans Kaspersky Security Center.

2. Mettez à jour les applications EPP conformément aux exigences :

- Kaspersky Endpoint Security for Windows – version 12.6 ou ultérieure
- Kaspersky Endpoint Security for Windows version 12.6 ou ultérieure, le mode Endpoint Detection and Response Agent (nécessite l'installation d'un fichier BLOB)
- Kaspersky Endpoint Security for Windows Light Agent – version 12.8 ou ultérieure
- Kaspersky Endpoint Security for Linux – version 12.3 ou ultérieure
- Kaspersky Endpoint Security for Mac version 12.2 ou ultérieure
- Kaspersky Embedded Systems Security for Windows – version 4.0 ou ultérieure
- Kaspersky Industrial CyberSecurity for Nodes Windows 4.5

3. Désactivez l'utilisation de KPSN dans le Serveur d'administration.

- Dans Kaspersky Security Center qui utilise le plug-in MDR :

1. Assurez-vous que le plug-in MDR est mis à jour vers la version 2.5.1.

2. Pour ce faire, dans la section MDR de la fenêtre de Kaspersky Security Center, cliquez sur l'onglet **Utilisation de MDR**.

3. Développez le bloc **KPSN** et cliquez sur **Désactiver KPSN**.

- Dans Kaspersky Security Center, qui n'utilise pas le plug-in MDR :

1. Dans le menu principal, cliquez sur l'icône des paramètres () à côté du nom du Serveur d'administration requis.

2. La fenêtre des propriétés du Serveur d'administration s'ouvre.

3. Sous l'onglet **Général**, sélectionnez la section Paramètres du proxy KSN.

4. Désactivez l'option **Utiliser Kaspersky Private Security Network**.

5. Activez l'option **Activer le proxy KSN sur le Serveur d'administration**.

4. Si vous déployez des ressources à partir d'une image de système d'exploitation, mettez à jour l'image afin que l'application EPP n'utilise pas la configuration KPSN.

5. Modifiez les stratégies pour les applications EPP (nécessaires pour les scénarios d'utilisation du code d'activation et du fichier BLOB).
 1. Désactivez l'utilisation de Kaspersky Security Network et enregistrez la stratégie. Consultez l'article [Configuration de Kaspersky Security Network](#)  pour en savoir plus.
 2. Si l'application EPP ne peut être activée qu'avec un fichier BLOB, [téléchargez le fichier de configuration MDR](#) et chargez le fichier BLOB dans la stratégie.
 3. Réactivez l'utilisation de Kaspersky Security Network et acceptez le contrat KSN. Assurez-vous que l'option Appliquer est activée dans les paramètres de la stratégie.

Tableaux de bord de surveillance dans de la Console MDR en ligne

La Console MDR en ligne propose des tableaux de bord de surveillance pour consulter des informations synthétiques.

Pour afficher les tableaux de bord :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Monitoring**.

La page **Summary** s'ouvre.

2. Les tableaux de bord suivants sont présents sur la page **Summary** :

- **Number of connected assets**

Cette section présente le nombre de ressources connectées par rapport au nombre cible de ressources.

- **Assets by status**

Il s'agit d'un diagramme circulaire qui présente la répartition des ressources, selon leurs états.

- **Active incidents**

Il s'agit d'un diagramme circulaire qui présente la répartition des incidents ressources, selon leurs états.

- **Responses**

Il s'agit d'un diagramme circulaire qui présente la répartition des réponses, selon leurs états.

Le nombre des ressources connectées représente les ressources qui ont été vues dans la Console MDR en ligne au cours des 7 derniers jours. Si vous souhaitez obtenir le nombre de ressources connectées pour la période précisée, accédez à l'option du menu **Assets** de la Console MDR en ligne.

- **Telemetry statistics**

Il s'agit d'un tableau de bord qui affiche les statistiques de télémétrie de la solution MDR pour un client, y compris les statistiques par locataire spécifique. Vous pouvez visualiser les données pour 1 jour, 7, 30, 90, 180 jours, 1 an, ou pour toute la période pendant laquelle un client utilise la solution MDR en continu.

Ce tableau de bord affiche le nombre de chacun des objets suivants :

- Les *Telemetry events** sont tous les événements envoyés par les ressources d'un client à Kaspersky Managed Detection and Response.
- *Suspicious events* sont des événements de télémétrie que Kaspersky Managed Detection and Response considère comme des événements nécessitant une vérification complémentaire.
- Les *Security events* sont des événements de télémétrie que les règles de détection déterminent comme des incidents potentiels.

- Les *Incidents* sont des actions jugées critiques par la technologie de détection. Les incidents requièrent une réaction immédiate (action de réaction) de Kaspersky Managed Detection and Response.
- *Detection rules triggered* correspondent à un nombre de règles de détection uniques déclenchées pour des événements de télémétrie spécifiés pendant une période donnée.

Les tableaux de bord sont mis à jour à chaque actualisation de la page **Summary**.

Pour basculer les tableaux de bord vers des statistiques spécifiques au locataire :

1. En haut de la page **Summary**, cliquez sur **Filtrer**.
2. Dans le menu appelé, sélectionnez un ou plusieurs locataires.
3. Cliquez sur **Save**.

Des statistiques spécifiques aux locataires sont disponibles pour les widgets suivants :

- **Assets limit for this license**
- **Assets by status**
- **Active incidents**
- **Incidents**
- **Responses**
- **Telemetry statistics**

Réception d'informations récapitulatives

Kaspersky Managed Detection and Response fournit plusieurs types d'informations récapitulatives que vous pouvez recevoir par e-mail. Cette section décrit comment configurer la réception des informations récapitulatives.

Recevoir un résumé de toutes les ressources sous forme de fichier CSV (Console MDR en ligne)

Vous pouvez recevoir un résumé sous la forme d'un fichier CSV contenant toutes les ressources de votre compte. Aucun filtre n'est appliqué au résumé, c'est-à-dire que le nombre des ressources dans ce résumé représente toutes les ressources qui s'affichent dans la Console MDR en ligne.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans le résumé en cochant la case correspondante dans les **Paramètres**.

Pour recevoir un résumé au format CSV, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Assets**.
La liste des appareils s'ouvre.
2. Cliquez sur le bouton **Receive a CSV summary by email** par e-mail dans la partie supérieure de la fenêtre.

Le résumé est envoyé à l'adresse e-mail que vous avez indiquée lors de l'activation de Kaspersky Managed Detection and Response.

Réception des informations sur l'incident au format PDF (Console MDR en ligne)

Vous pouvez recevoir un résumé des informations relatives à un incident particulier au format PDF.

Pour recevoir un résumé PDF, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Incidents**.
La liste des incidents s'ouvre.
2. Cliquez sur l'incident dont vous souhaitez recevoir le résumé.
La carte d'incident s'affiche.
3. Cliquez sur le lien **Receive a PDF by email** dans la partie supérieure de la fenêtre.

Le résumé est envoyé à l'adresse e-mail que vous avez indiquée lors de l'activation de Kaspersky Managed Detection and Response.

Configuration de l'envoi régulier de rapports dans la Console MDR en ligne

Cette fonctionnalité est disponible uniquement dans la Console MDR en ligne.

Vous pouvez configurer la réception d'un rapport de synthèse contenant les données sur les incidents en cours. Chaque ensemble de paramètres de livraison est enregistré sous la forme d'un calendrier. Vous pouvez créer un maximum de 50 calendriers pour une organisation et un maximum de 10 calendriers pour chaque client.

Pour créer ou modifier les calendriers de remise des rapports, vous devez disposer du [rôle utilisateur Administrateur MDR](#).

Le rapport est envoyé par e-mail au format PDF ouvert et non chiffré aux adresses que vous avez indiquées et selon la programmation définie.

Le rapport contient toujours les données des sept derniers jours. Le jour de la création du rapport n'est pas inclus. En d'autres termes, si vous effectuez la configuration de manière à recevoir le rapport de synthèse tous les jours, votre rapport quotidien contiendra les données des sept derniers jours, sauf le jour actuel. Si vous configurez la réception du rapport de synthèse tous les mercredis, le rapport contiendra les données du mercredi précédent au mardi suivant.

Pour configurer la réception de la synthèse du rapport au format PDF, procédez comme suit :

1. Dans la section **Settings** de la Console MDR en ligne, cliquez sur l'onglet **Schedules**.

2. Cliquez sur le bouton **Add**.

La fenêtre **Add new schedule** s'ouvre.

3. Mettez bouton à bascule en position **Enabled**.

4. Lisez attentivement la notification ci-dessous relative aux conditions d'envoi des rapports de synthèse. Ensuite, cochez la case pour confirmer que vous avez lu et compris les conditions d'utilisation. Si la case n'est pas cochée, vous ne pouvez pas enregistrer les modifications.

5. Spécifiez les paramètres suivants :

- Dans le champ **Schedule name**, indiquez un nom arbitraire et lisible pour le rapport de synthèse. Le nom doit contenir des lettres latines, des chiffres et des caractères spéciaux ; il ne peut pas comporter plus de 1000 caractères.
- Dans le champ **Tenant**, sélectionnez le locataire pour lequel vous souhaitez recevoir un rapport de synthèse. Le rapport contient uniquement les données du locataire sélectionné. Sinon, si vous souhaitez recevoir un rapport de synthèse sur tous les locataires, sélectionnez **All tenants**.

- Dans le champ **To emails**, indiquez l'adresse e-mail ou la liste, séparées par des virgules, des adresses e-mail des utilisateurs qui recevront le résumé.

Vérifiez bien les adresses e-mail saisies, car elles seront ajoutées sans autre confirmation. Les rapports de synthèse peuvent contenir des données sensibles et sont envoyés au format PDF ouvert et non chiffré.

- Dans le champ **Sending day**, sélectionnez les jours de la semaine où le résumé doit être envoyé aux adresses e-mail indiquées. Vous pouvez choisir un jour ou **Every day**.
- Dans le champ **Time, UTC**, indiquez l'heure au format UTC 24 heures. Par exemple, 15 h 00.

Le calendrier affecte uniquement l'heure de réception du rapport, mais n'affecte pas la période de données dans le rapport.

Le rapport contient toujours les données des sept derniers jours. Le jour de la création du rapport n'est pas inclus. En d'autres termes, si vous effectuez la configuration de manière à recevoir le rapport de synthèse tous les jours, votre rapport quotidien contiendra les données des sept derniers jours, sauf le jour actuel. Si vous configurez la réception du rapport de synthèse tous les mercredis, le rapport contiendra les données du mercredi précédent au mardi suivant.

6. Cliquez sur le bouton **Enregistrer**.

Le rapport de synthèse sera envoyé aux adresses e-mail sur une base hebdomadaire ou quotidienne.

Réception de notifications

Vous pouvez configurer l'envoi de notifications sur les événements qui se produisent avec les incidents et les réponses au fur et à mesure de leur traitement dans Kaspersky Managed Detection and Response.

Kaspersky Managed Detection and Response envoie des notifications aux clients via Telegram ou par e-mail, en fonction des paramètres que vous avez définis. Le corps de notification contient une description de l'événement et un lien vers l'objet sur lequel l'événement s'est produit.

Vous pouvez configurer les notifications dans la Console MDR en ligne.

Configuration des notifications dans la Console MDR en ligne

Pour configurer l'envoi des notifications dans la Console MDR en ligne procédez comme suit :

1. Dans la section **Settings** de la Console MDR en ligne, cliquez sur l'onglet **Notification settings**.
2. Cochez les cases correspondant aux événements pour lesquels vous souhaitez recevoir des notifications par e-mail ou dans Telegram.

Voici les cases à cocher disponibles :

- **All** : tous les événements à propos desquels Kaspersky Managed Detection and Response envoie des notifications.
 - **Incidents** : notifications relatives à la création, la mise à jour, la résolution et la clôture des incidents.
 - **Extended notifications** : une description de l'attaque détectée comme incident et les recommandations de réponse. Cette case est disponible si la fonctionnalité de notifications détaillées est [activée sous l'onglet General settings](#). Ces notifications peuvent être activées uniquement dans la Console MDR en ligne, mais pas dans le plug-in MDR.
 - **Comments** : notifications relatives à la création, à la mise à jour et à la suppression de commentaires dans les incidents.
 - **Responses** : notifications relatives à la création, à l'acceptation et au refus des réponses.
 - **Information on license expiration** : notifications relatives aux événements suivants : moins de 30 jours avant l'expiration de la licence, la licence a expiré. Kaspersky Managed Detection and Response envoie ces notifications tous les jours, mais pas après l'expiration ou le renouvellement de la licence.
3. Cliquez sur le bouton **Subscribe** situé au-dessus des cases à cocher pour vous abonner aux notifications du chatbot Telegram. Lorsque vous cliquez sur le bouton **Subscribe**, l'application génère un lien unique pour activer le chatbot dans Telegram. Vous pouvez utiliser ce lien pour un seul compte Telegram.

Utilisez ce lien uniquement sur un appareil (ordinateur de bureau ou mobile) sur lequel l'application Telegram est installée. Le lien ne peut pas activer le chatbot dans la version Internet de Telegram.

Si vous souhaitez recevoir des notifications sur un autre compte Telegram, cliquez sur le bouton **Unsubscribe**, puis répétez la procédure d'abonnement pour générer un nouveau lien et l'utiliser pour activer le chatbot pour un autre compte.

4. Cliquez sur le bouton **Save** dans la partie inférieure de la fenêtre pour enregistrer les paramètres. Le bouton **Save** ne devient actif que si vous avez modifié les paramètres.

La livraison des notifications est configurée.

Notifications sur l'état des ressources

Vous pouvez configurer l'envoi de notifications lorsqu'un nombre de ressources ayant un état spécifique dépasse un seuil.

Les notifications sur l'état des ressources vous permettent de recevoir en temps opportun des informations sur les problèmes suivants :

- Diminution de la couverture de la surveillance MDR
- Problèmes de connexion des ressources à MDR
- Passage massif des ressources à l'état Avertissement ou Critique

Pour en savoir plus sur les états des ressources, consultez l'article suivant : [États des ressources](#).

Fonctionnement des notifications automatiques

Pour chacun des états répertoriés ci-dessous, vous pouvez définir une valeur seuil sous forme de pourcentage du nombre total de ressources. Lorsque le seuil est dépassé, une notification est envoyée.

État	Condition
OK	Le nombre de ressources est inférieur au seuil.
Attention	Le nombre de ressources est supérieur au seuil.
Critique	Le nombre de ressources est supérieur au seuil.
Hors ligne	Le nombre de ressources est supérieur au seuil.

Les vérifications automatiques des ressources sont effectuées à un intervalle de 1 heure.

Les notifications sont envoyées séparément pour chaque locataire qui dépasse ses seuils. Une notification pour un état donné est envoyée au maximum une fois par jour et par locataire.

Seuls les utilisateurs ayant accès au locataire dont les seuils sont dépassés et ayant activé les notifications dans leurs paramètres utilisateur reçoivent les notifications.

Configuration des règles de notification par l'Administrateur MDR

La configuration des notifications sur l'état des ressources requiert le rôle d'Administrateur MDR.

Pour configurer les règles de notification sur l'état des ressources :

1. Dans la console MDR, accédez à **Paramètres** → **Paramètres généraux**.
2. Activez l'une des options suivantes ou les deux :
 - **Recevoir des notifications détaillées par email**
 - **Recevoir des notifications détaillées par Telegram**
3. Activez le paramètre **Activer les notifications en cas de modification de l'état des ressources**.

Le panneau **Règle de base** devient modifiable et contient les paramètres de la règle de notification. Vous pouvez ajouter des règles supplémentaires (par exemple, pour un autre ensemble de locataires) en cliquant sur le bouton **Ajouter une règle** sous le panneau **Règle de base**.
4. Dans le panneau, sélectionnez les locataires auxquels la règle s'appliquera ou activez l'option **Appliquer à tous les locataires**.
5. Définissez les valeurs seuils des états des ressources ou conservez les valeurs par défaut.
6. Cliquez sur **Enregistrer**.

La règle est maintenant créée et active. Pour recevoir des notifications, les utilisateurs MDR doivent configurer les notifications sur l'état des ressources comme décrit ci-dessous.

Configuration des notifications sur l'état des ressources par les utilisateurs MDR

Pour recevoir les notifications sur l'état des ressources :

1. Dans la console MDR, accédez à **Paramètres** → **Paramètres de notification**.
2. Activez les **notifications sur l'état des ressources**.
3. Cliquez sur **Enregistrer**.

Vous recevrez désormais les notifications sur l'état des ressources pour les locataires auxquels vous avez accès, conformément aux règles configurées.

Réception de notifications étendues

Vous pouvez configurer l'envoi de notifications détaillées d'incidents par e-mail ou Telegram aux utilisateurs MDR. Les notifications détaillées contiennent une description de l'attaque détectée comme incident et les recommandations de réponse. La description de l'attaque comporte des données que la solution MDR reçoit sous forme de télémétrie à partir d'appareils connectés à la solution MDR. Elle peut donc inclure les informations sensibles suivantes :

- Noms des hôtes
- Adresses IP des hôtes
- Noms des comptes
- Mots de passe des comptes (si le script contenant le mot de passe a été exécuté sur l'appareil)
- URL des services
- Noms des fichiers
- Adresses e-mail
- Noms des services et des locataires

La liste complète des données reçues par la solution MDR est présentée dans la section [Collecte des données](#).

Activation des notifications détaillées dans la Console MDR en ligne

Pour activer la remise des notifications détaillées, procédez comme suit :

1. Dans la section **Settings** de la Console MDR en ligne, cliquez sur l'onglet **General settings**.
2. Activez une ou les deux options :
 - **Enable extended email notification**
 - **Enable extended Telegram notification**
3. Cochez la case en bas du panneau pour confirmer que vous avez lu et compris les conditions d'envoi des notifications détaillées.
4. Cliquez sur **Save**.

Vous pouvez désormais [vous abonner](#) aux notifications détaillées dans les **Notification settings** de la Console MDR en ligne.

Administration des utilisateurs

Les utilisateurs de Kaspersky Managed Detection and Response peuvent présenter différents rôles, avec une fonctionnalité différente disponible pour chaque rôle. Le *modèle de rôle* est un ensemble de règles qui précisent les rôles des utilisateurs.

Les rôles suivants sont présents dans Kaspersky Managed Detection and Response :

MDR Administrator

Le superutilisateur qui a accès à l'ensemble des fonctions de Kaspersky Managed Detection and Response accordées par la licence. L'administrateur MDR peut accorder l'accès aux sources de données client à d'autres utilisateurs. Lorsque vous activez Kaspersky Managed Detection and Response, vous devenez automatiquement l'administrateur MDR, c'est pourquoi, dans le cadre du processus d'activation, nous vous recommandons d'utiliser une adresse e-mail d'entreprise plutôt qu'une adresse e-mail personnelle. La création d'un compte d'administrateur MDR avec une adresse e-mail personnelle peut poser des risques de sécurité tels que le vol du compte d'administrateur MDR.

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	✓	—
Programmation du résumé des incidents	✓	—
Accès à l'API REST	✓	—

Senior Security Officer

Un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. L'Agent de sécurité principal a le droit d'accepter et de refuser des [réponses](#) ².

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

Security Officer

Un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. Le responsable de la sécurité ne peut ni accepter ni refuser des [réponses](#) ².

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	—	✓

Domaine fonctionnel	Autoriser	Refuser
Gestion des réponses	—	✓
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

Invitation de nouveaux utilisateurs dans la Console MDR en ligne

Pour inviter un nouvel utilisateur à Kaspersky Managed Detection and Response, procédez comme suit :

Si le compte [Kaspersky Account](#) créé précédemment (c'est-à-dire votre adresse e-mail) a déjà été utilisé pour accéder à Kaspersky Managed Detection and Response, il peut être associé aux données MDR d'une autre organisation et ne pas être disponible pour utiliser un nouveau code d'activation. Pour utiliser votre compte Kaspersky Account existant en vue d'une nouvelle activation, contactez le [Support Technique](#).
Remarque : lorsque le Support Technique supprime l'association de votre compte Kaspersky Account existant avec les données d'une autre organisation la solution MDR, celui-ci ne peut plus être utilisé pour accéder aux données de l'autre organisation pour lesquelles il était auparavant utilisé.

1. Dans la fenêtre de la Console MDR, accédez à l'option du menu **Settings**.

La liste des utilisateurs s'ouvre.

2. Cliquez sur le bouton **Add** situé au-dessus de la liste des utilisateurs.

La carte des invitations s'affiche.

3. Dans le champ **Email**, indiquez une adresse e-mail.

4. Dans le champ **User role**, indiquez un rôle pour le nouvel utilisateur.

Les rôles d'utilisateur suivants sont disponibles :

MDR Administrator

Le superutilisateur qui a accès à l'ensemble des fonctions de Kaspersky Managed Detection and Response accordées par la licence. L'administrateur MDR peut accorder l'accès aux sources de données client à d'autres utilisateurs. Lorsque vous activez Kaspersky Managed Detection and Response, vous devenez automatiquement l'administrateur MDR, c'est pourquoi, dans le cadre du processus d'activation, nous vous recommandons d'utiliser une adresse e-mail d'entreprise plutôt qu'une adresse e-mail personnelle. La création d'un compte d'administrateur MDR avec une adresse e-mail personnelle peut poser des risques de sécurité tels que le vol du compte d'administrateur MDR.

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	✓	—
Programmation du résumé des incidents	✓	—
Accès à l'API REST	✓	—

Seul l'utilisateur auquel le [rôle](#) d'**MDR Administrator** a été attribué peut attribuer le rôle d'**MDR Administrator** à un nouvel utilisateur.

Senior Security Officer

Un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. L'Agent de sécurité principal a le droit d'accepter et de refuser des [réponses](#) [?](#)

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

Security Officer

Un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. Le responsable de la sécurité ne peut ni accepter ni refuser des [réponses](#) [?](#)

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	—	✓
Gestion des réponses	—	✓
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

5. Si nécessaire, sélectionnez la valeur (ou les valeurs) dans la liste déroulante **Tenant**.

Les locataires existants et la valeur **Root tenant** sont proposés.

L'utilisateur peut afficher uniquement les ressources et les incidents liés aux locataires indiqués. Si vous avez des ressources et des incidents qui ne sont attribués à aucun locataire, l'utilisateur peut les afficher si vous sélectionnez la valeur **Root tenant**.

Vous pouvez sélectionner la valeur **Root tenant** en plus de préciser les noms des locataires.

6. Cliquez sur **Invite**.

La carte des invitations disparaît.

Saisissez l'adresse e-mail. L'adresse e-mail doit d'abord être enregistrée et vérifiée sur le portail Web auth.hq.uis.kaspersky.com.

Un message contenant le lien d'invitation est envoyé de l'adresse noreply@mail.account.uis.kaspersky.com à l'adresse e-mail indiquée.

L'utilisateur invité doit vérifier son adresse e-mail en suivant le lien présent dans le message. L'utilisateur ne peut pas se connecter et utiliser Kaspersky Managed Detection and Response tant que son adresse e-mail n'est pas vérifiée. Les autorisations correspondant au rôle d'utilisateur seront accordées après la première connexion de l'utilisateur.

Modification des rôles des utilisateurs dans la Console MDR en ligne

Vous pouvez modifier le rôle d'un utilisateur existant. Par exemple, un employé auquel le rôle Responsable de la sécurité se voit attribuer des responsabilités supplémentaires qui nécessitent l'attribution du rôle d'agent de sécurité principal.

Pour modifier un rôle pour un utilisateur existant, procédez comme suit :

1. Dans la fenêtre de la Console MDR, accédez à l'option du menu **Settings**.

La liste des utilisateurs s'ouvre.

2. Cliquez sur la chaîne contenant l'utilisateur dont vous souhaitez modifier le rôle.

La carte d'utilisateur s'affiche.

3. Dans la carte d'utilisateur, modifiez le rôle de l'utilisateur existant en sélectionnant un autre rôle dans la liste déroulante des rôles.

4. Cliquez sur **Enregistrer**.

Le rôle de l'utilisateur existant est modifié.

Modification des modes de notification des utilisateurs dans la Console MDR en ligne

La modification des méthodes de notification des utilisateurs n'est disponible que pour l'utilisateur auquel le [rôle](#) Administrateur MDR est attribué. L'utilisateur disposant de ce rôle peut modifier les paramètres de notification de tous les utilisateurs présentant l'état actif, y compris les siens.

Les utilisateurs présentant l'état actif peuvent recevoir des notifications de Kaspersky Managed Detection and Response par e-mail et/ou via Telegram.

Pour modifier les méthodes de notification des utilisateurs pour un utilisateur existant, procédez comme suit :

1. Dans la fenêtre de la Console MDR, accédez à l'option du menu **Settings**.

La liste des utilisateurs s'ouvre.

2. Cliquez sur la chaîne contenant l'utilisateur dont vous souhaitez modifier les méthodes de notification.

La carte d'utilisateur s'affiche.

3. Dans la carte d'utilisateur, indiquez les options suivantes :

- **Email notifications enabled**

L'utilisateur reçoit des notifications à l'adresse e-mail indiquée lorsque cet utilisateur a été invité.

- **Telegram notifications enabled**

L'utilisateur reçoit des notifications du chatbot Telegram.

Si un utilisateur n'a plus accès au compte Telegram, cochez la case **Unsubscribe Telegram account from notifications**. Demandez ensuite à l'utilisateur de se connecter à la Console MDR en ligne, accédez à **Settings** → **Notification settings** et répétez la procédure d'abonnement pour générer un nouveau lien afin d'activer l'abonnement pour un autre compte Telegram.

4. Dans la partie inférieure de la carte utilisateur, cliquez sur le bouton **Save** pour fermer la carte.

Les méthodes de notifications des utilisateurs sont modifiées et enregistrées.

Modification de l'accès des utilisateurs aux clients dans la Console MDR en ligne

Vous pouvez modifier l'accès des utilisateurs aux locataires de votre compte, par exemple, si vous ajoutez un nouveau locataire et souhaitez qu'un utilisateur existant y ait accès.

Pour modifier l'accès aux locataires, procédez comme suit :

1. Dans la fenêtre de la Console MDR, accédez à l'option du menu **Settings**.

La liste des utilisateurs s'ouvre.

2. Cliquez sur la chaîne contenant l'utilisateur dont vous souhaitez modifier les droits d'accès.

La carte d'utilisateur s'affiche.

3. Dans la carte d'utilisateur, modifiez la valeur (ou les valeurs) dans la liste déroulante **Tenant**.

4. Dans la partie inférieure de la carte utilisateur, cliquez sur le bouton **Save** pour fermer la carte.

L'accès des utilisateurs aux locataires est modifié.

Suppression de comptes utilisateurs

La suppression de comptes utilisateurs est disponible dans la console MDR et sur le site Internet de Kaspersky.

Suppression de comptes utilisateurs MDR dans la console MDR

Le compte Administrateur MDR est requis pour supprimer des comptes utilisateurs MDR.

L'adresse email associée à un compte supprimé ne reçoit plus de notifications ni de rapports. Pour restaurer l'accès à la console MDR, [une nouvelle invitation doit être envoyée à l'adresse email](#).

Lorsque vous ne disposez que d'un seul compte Administrateur MDR, ce compte ne peut pas être supprimé.

Pour supprimer un compte utilisateur MDR :

1. Dans la fenêtre de la Console MDR, accédez à l'option du menu **Settings**.

La liste des utilisateurs s'ouvre.

2. Dans la liste des utilisateurs, placez le pointeur de la souris sur l'utilisateur que vous souhaitez supprimer, puis cliquez sur l'icône de corbeille située à droite.

La fenêtre **Confirm user deletion** s'affiche.

3. Cliquez sur le bouton **Delete** pour supprimer l'utilisateur.

Suppression de comptes Kaspersky Account

Les utilisateurs peuvent supprimer leur propre Kaspersky Account sur le site Internet de Kaspersky, quels que soient les droits utilisateur qui leur sont attribués.

La suppression d'un Kaspersky Account entraîne automatiquement celle du compte utilisateur MDR correspondant. L'adresse email associée au Kaspersky Account supprimé ne reçoit plus les notifications ni les rapports MDR.

Si tous les comptes utilisateurs des Administrateurs MDR sont supprimés, il n'est plus possible d'ajouter de nouveaux utilisateurs ni de configurer la console MDR. Dans ce cas, [contactez le Support technique](#).

Si vous supprimez le Kaspersky Account utilisé pour configurer le plug-in MDR sur le Serveur d'administration ou Open Single Management Platform, le plug-in MDR doit être reconfiguré.

Gestion des éléments

Une *ressource* est un appareil sur lequel est installée une application Kaspersky EPP (par exemple, Kaspersky Endpoint Security for Windows). Cette section fournit des informations sur l'affichage, le tri et le filtrage des ressources.

Affichage et recherche dans les ressources de la Console MDR en ligne

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Vous pouvez afficher et effectuer des recherches dans les ressources disponibles en utilisant la liste des ressources.

Pour afficher les ressources :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Assets**.

La liste des ressources s'ouvre. Chaque ligne représente une ressource. Vous pouvez cliquer n'importe où sur la ligne pour afficher les informations à propos de la ressource.

Les attributs des ressources suivants peuvent être affichés au-dessus de la liste :

Asset name

Le nom d'un ordinateur sur le réseau.

Vous pouvez cliquer sur **Asset name** pour afficher les informations relatives à la ressource dans Kaspersky Security Center Web Console.

Asset ID

Identifiant unique d'une ressource. L'identifiant de la ressource est généré automatiquement par Kaspersky Managed Detection and Response avant que la ressource envoie la télémétrie pour la première fois.

Applications

Application EPP installée sur la ressource et configurée pour être utilisée avec Kaspersky Managed Detection and Response.

Interfaces

Nombre de toutes les interfaces réseau disponibles sur l'appareil.

Operating system

Système d'exploitation installé sur la ressource.

Domain

Un domaine de réseau auquel appartient la ressource.

Tenant

Le nom du [locataire](#), si la ressource appartient à l'un des locataires. Si la ressource n'appartient pas à un locataire, ce champ est vide.

Last seen

Nombre de jours écoulés depuis la dernière fois que la ressource a été consultée dans la Console MDR en ligne.

Les ressources sont triées en fonction de cet attribut, par ordre décroissant.

Par défaut, les ressources qui ont été vues au cours des 30 derniers jours sont affichées. Vous pouvez étendre la période en filtrant les ressources.

Status

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

L'état reflète l'état actuel de la ressource. Pour les ressources présentant l'état *OK*, *Avertissement* ou *Critique*, l'application répertorie en plus les problèmes rencontrés (le cas échéant) au cours des 72 dernières heures.

Les ressources présentent l'un des états suivants :

- **OK** (vert)

La télémétrie est envoyée, la protection est entièrement opérationnelle.

- **Warning** (jaune)

Raisons possibles de l'état **Warning** :

- Pertes de télémétrie mineures. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Les bases de données antivirus sont obsolètes depuis plus de 7 jours.
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

Pare-feu

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces réseau

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 

- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces par emails et extension supplémentaire pour Microsoft Office Outlook

L'article suivant explique comment activer ou configurer ce module : [Kaspersky Endpoint Security for Windows](#) .

Protection contre les menaces Internet

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

Composant autodéfense du produit

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Ces composants ont une incidence sur l'exhaustivité des données de télémétrie envoyées. Si un composant est désactivé ou manquant, Kaspersky Managed Detection and Response n'envoie pas les événements de télémétrie liés à ce composant. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN arrive à expiration. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#). Si vous continuez à utiliser le fichier de configuration actuel, l'état devient **Critical** quelques jours avant la date d'expiration.

L'état **Warning** s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization Light Agent 5.2 ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Critical** (rouge)

Raisons possibles de l'état **Critical** :

- Pertes de télémétrie majeures, les données de télémétrie sont insuffisantes pour l'analyse. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

- **Surveillance du système ou Détection comportementale**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Protection contre les fichiers malicieux**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si l'un de ces composants est désactivé ou manquant, Kaspersky Managed Detection and Response interrompt l'envoi de télémétrie à partir de la ressource. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN expire bientôt ou a déjà expiré. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#).

Cet état s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization 5.2 Light Agent ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Offline** (noir)

Pas de télémétrie pendant plus de 7 jours (valeur par défaut). Dans la section **Paramètres**, vous pouvez modifier le nombre de jours d'absence de la télémétrie après lequel l'état **Offline** de la ressource s'affiche. La période peut aller de 2 à 29 jours.

Si l'état **Offline** apparaît pour vos ressources, procédez comme suit :

- Assurez-vous que les modules de l'application EPP répertoriés dans les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

L'état **Offline** ne s'applique pas aux ressources VDI (machines virtuelles temporaires).

- **Absent** (noir)

Absence de télémétrie pendant plus de 30 jours pour les ressources physiques ou pendant plus de 24 heures pour les ressources VDI (machines virtuelles temporaires).

Si l'état **Absent** s'affiche pour vos ressources :

- Assurez-vous que les modules de l'application EPP présentant les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans [la liste des ressources](#), dans [les rapports](#) et dans les données reçues via [l'interface API](#).

En haut de la liste des incidents se trouvent les boutons suivants :

- Le bouton **Columns** avec l'icône en forme de roue dentée permettant de sélectionner les colonnes à afficher dans l'onglet **History**.
- Le bouton **Filter** avec l'icône en forme d'entonnoir pour afficher les modifications liées uniquement aux cases sélectionnées.
- Le bouton **Search** avec l'icône en forme de loupe permet d'afficher les modifications liées uniquement aux mots ou aux caractères saisis.

2. Si vous souhaitez modifier le nombre de ressources affichées par page de la liste, sélectionnez le nombre en cliquant sur l'option **entries per page** au bas de la page.

Vous pouvez sélectionner 10, 20 ou 50 ressources par page.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans la liste des ressources en cochant la case correspondante dans l'onglet **Settings** → **General settings**.

Si vous souhaitez parcourir la liste des ressources, sélectionnez la page en dessous de la liste. Vous pouvez utiliser les options **Previous** et **Next** pour basculer entre les pages adjacentes.

Par défaut, la liste des ressources contient celles qui ont été affichées dans la Console MDR en ligne au cours des 30 derniers jours.

Pour modifier cette période, procédez comme suit :

1. Cliquez sur l'icône en forme d'entonnoir au-dessus de la liste.
2. Dans le panneau **Filter** situé à droite, sélectionnez la période dans le champ **Last seen**.
3. Cliquez sur **Save**.

Vous pouvez effectuer une recherche parmi les ressources en cliquant sur l'icône en forme de loupe située à côté de l'icône d'entonnoir au-dessus de la liste des ressources.

Filtrage des ressources dans la Console MDR en ligne

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Vous pouvez créer et appliquer des filtres à la liste des ressources.

Pour créer un filtre pour la liste des ressources, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Assets**.
La liste des appareils s'ouvre.
2. Cliquez sur l'icône d'entonnoir située au-dessus de la liste des ressources.
Le menu **Filter** s'affiche.
Voici les paramètres disponibles pour le filtrage :

- **Last seen**

Moment où la ressource a été vue pour la dernière fois dans la Console MDR en ligne.

- **Asset name**

Noms des ressources disponibles.

Le nom de la ressource est le nom d'un ordinateur sur le réseau.

- **Tenant**

Noms de locataires disponibles.

Vous pouvez sélectionner la valeur **Root tenant** pour afficher les ressources qui ne sont attribuées à aucun de vos locataires.

Vous pouvez sélectionner la valeur **Root tenant** en plus de préciser les noms des locataires.

- **Status**

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

L'état reflète l'état actuel de la ressource. Pour les ressources présentant l'état *OK*, *Avertissement* ou *Critique*, l'application répertorie en plus les problèmes rencontrés (le cas échéant) au cours des 72 dernières heures.

Les ressources présentent l'un des états suivants :

- **OK** (vert)

La télémétrie est envoyée, la protection est entièrement opérationnelle.

- **Warning** (jaune)

Raisons possibles de l'état **Warning** :

- Pertes de télémétrie mineures. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Les bases de données antivirus sont obsolètes depuis plus de 7 jours.
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

Pare-feu

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces réseau

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces par emails et extension supplémentaire pour Microsoft Office Outlook

L'article suivant explique comment activer ou configurer ce module : [Kaspersky Endpoint Security for Windows](#) .

Protection contre les menaces Internet

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

Composant autodéfense du produit

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Ces composants ont une incidence sur l'exhaustivité des données de télémétrie envoyées. Si un composant est désactivé ou manquant, Kaspersky Managed Detection and Response n'envoie pas les événements de télémétrie liés à ce composant. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN arrive à expiration. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#). Si vous continuez à utiliser le fichier de configuration actuel, l'état devient **Critical** quelques jours avant la date d'expiration.

L'état **Warning** s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization Light Agent 5.2 ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Critical** (rouge)

Raisons possibles de l'état **Critical** :

- Pertes de télémétrie majeures, les données de télémétrie sont insuffisantes pour l'analyse. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :
 - **Surveillance du système ou Détection comportementale**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 

- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Protection contre les fichiers malicieux**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si l'un de ces composants est désactivé ou manquant, Kaspersky Managed Detection and Response interrompt l'envoi de télémétrie à partir de la ressource. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN expire bientôt ou a déjà expiré. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#).

Cet état s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization 5.2 Light Agent ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Offline** (noir)

Pas de télémétrie pendant plus de 7 jours (valeur par défaut). Dans la section **Paramètres**, vous pouvez modifier le nombre de jours d'absence de la télémétrie après lequel l'état **Offline** de la ressource s'affiche. La période peut aller de 2 à 29 jours.

Si l'état **Offline** apparaît pour vos ressources, procédez comme suit :

- Assurez-vous que les modules de l'application EPP répertoriés dans les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

L'état **Offline** ne s'applique pas aux ressources VDI (machines virtuelles temporaires).

- **Absent** (noir)

Absence de télémétrie pendant plus de 30 jours pour les ressources physiques ou pendant plus de 24 heures pour les ressources VDI (machines virtuelles temporaires).

Si l'état **Absent** s'affiche pour vos ressources :

- Assurez-vous que les modules de l'application EPP présentant les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est correctement déployé dans votre infrastructure.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans la liste des ressources, dans les rapports et dans les données reçues via l'interface API.

- **Isolation**

Indique si l'isolement du réseau est activé ou non. Les valeurs de filtre possibles sont les suivantes :

- **Isolated**

L'isolement du réseau est activé.

- **Not isolated**

L'isolement du réseau est désactivé.

3. Cliquez sur **Save** pour appliquer le filtre créé.

Une fois que le filtre est appliqué, seuls les ressources qui répondent aux paramètres sélectionnés du filtre sont affichées dans la liste des ressources.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans la liste des ressources en cochant la case correspondante dans l'onglet **Settings** → **General settings**.

Affichage d'informations détaillées concernant les ressources dans la Console MDR en ligne

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Pour afficher des informations détaillées sur les ressources, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Assets**.

La liste des appareils s'ouvre.

2. Cliquez sur la chaîne présentant la ressource dont vous souhaitez afficher les détails.

La liste des ressources s'affiche. La carte des ressources contient deux onglets :

- L'onglet **Properties** contient des informations générales sur la ressource
- L'onglet **Incidents** contient des informations sur les incidents qui se sont produits avec la ressource

L'onglet **Properties** contient les informations suivantes :

- **Asset name**

Le nom d'un ordinateur sur le réseau.

Vous pouvez cliquer sur **Asset name** pour afficher les informations relatives à l'appareil dans Kaspersky Security Center Web Console.

- **Status**

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

L'état reflète l'état actuel de la ressource. Pour les ressources présentant l'état *OK*, *Avertissement* ou *Critique*, l'application répertorie en plus les problèmes rencontrés (le cas échéant) au cours des 72 dernières heures.

Les ressources présentent l'un des états suivants :

- **OK** (vert)

La télémétrie est envoyée, la protection est entièrement opérationnelle.

- **Warning** (jaune)

Raisons possibles de l'état **Warning** :

- Pertes de télémétrie mineures. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Les bases de données antivirus sont obsolètes depuis plus de 7 jours.
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

Pare-feu

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces réseau

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 

- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces par emails et extension supplémentaire pour Microsoft Office Outlook

L'article suivant explique comment activer ou configurer ce module : [Kaspersky Endpoint Security for Windows](#) .

Protection contre les menaces Internet

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

Composant autodéfense du produit

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Ces composants ont une incidence sur l'exhaustivité des données de télémétrie envoyées. Si un composant est désactivé ou manquant, Kaspersky Managed Detection and Response n'envoie pas les événements de télémétrie liés à ce composant. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN arrive à expiration. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#). Si vous continuez à utiliser le fichier de configuration actuel, l'état devient **Critical** quelques jours avant la date d'expiration.

L'état **Warning** s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization Light Agent 5.2 ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Critical** (rouge)

Raisons possibles de l'état **Critical** :

- Pertes de télémétrie majeures, les données de télémétrie sont insuffisantes pour l'analyse. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

- **Surveillance du système ou Détection comportementale**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Protection contre les fichiers malicieux**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si l'un de ces composants est désactivé ou manquant, Kaspersky Managed Detection and Response interrompt l'envoi de télémétrie à partir de la ressource. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN expire bientôt ou a déjà expiré. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#).

Cet état s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization 5.2 Light Agent ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#), , cet état n'est pas affiché.

- **Offline** (noir)

Pas de télémétrie pendant plus de 7 jours (valeur par défaut). Dans la section **Paramètres**, vous pouvez modifier le nombre de jours d'absence de la télémétrie après lequel l'état **Offline** de la ressource s'affiche. La période peut aller de 2 à 29 jours.

Si l'état **Offline** apparaît pour vos ressources, procédez comme suit :

- Assurez-vous que les modules de l'application EPP répertoriés dans les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

L'état **Offline** ne s'applique pas aux ressources VDI (machines virtuelles temporaires).

- **Absent** (noir)

Absence de télémétrie pendant plus de 30 jours pour les ressources physiques ou pendant plus de 24 heures pour les ressources VDI (machines virtuelles temporaires).

Si l'état **Absent** s'affiche pour vos ressources :

- Assurez-vous que les modules de l'application EPP présentant les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans [la liste des ressources](#), dans [les rapports](#) et dans les données reçues via [l'interface API](#).

- **IP address**

L'adresse IP de la ressource.

- **Physical address**

- **Tenant**

Le nom du [locataire](#), si la ressource appartient à l'un des locataires. Si la ressource n'appartient pas à un locataire, ce champ est vide.

- **First seen**

- **Last seen**

- **Operating system**

Système d'exploitation installé sur l'appareil.

- **Kaspersky applications that work with MDR**

- **Domain**

L'onglet **Incidents** contient la liste des incidents. La colonne **ID/Created** de la liste contient un identifiant d'incident et l'heure à laquelle l'incident a été créé. La colonne **Status** de la liste contient des informations sur l'état de l'incident.

États des ressources

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

L'état reflète l'état actuel de la ressource. Pour les ressources présentant l'état *OK*, *Avertissement* ou *Critique*, l'application répertorie en plus les problèmes rencontrés (le cas échéant) au cours des 72 dernières heures.

Les ressources présentent l'un des états suivants :

- **OK** (vert)

La télémétrie est envoyée, la protection est entièrement opérationnelle.

- **Warning** (jaune)

Raisons possibles de l'état **Warning** :

- Pertes de télémétrie mineures. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Les bases de données antivirus sont obsolètes depuis plus de 7 jours.
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

Pare-feu

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) [☞]
- [Kaspersky Security for Virtualization Light Agent](#) [☞]
- [Kaspersky Embedded Systems Security for Windows](#) [☞]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [☞]

Protection contre les menaces réseau

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) [☞]
- [Kaspersky Endpoint Security for Linux](#) [☞]
- [Kaspersky Endpoint Security for Mac](#) [☞]
- [Kaspersky Embedded Systems Security for Windows](#) [☞]
- [Kaspersky Embedded Systems Security for Linux](#) [☞]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [☞]

Protection contre les menaces par emails et extension supplémentaire pour Microsoft Office Outlook

L'article suivant explique comment activer ou configurer ce module : [Kaspersky Endpoint Security for Windows](#) [▢].

Protection contre les menaces Internet

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) [▢]
- [Kaspersky Endpoint Security for Linux](#) [▢]
- [Kaspersky Endpoint Security for Mac](#) [▢]
- [Kaspersky Security for Virtualization Light Agent](#) [▢]
- [Kaspersky Embedded Systems Security for Linux](#) [▢]

Composant autodéfense du produit

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) [▢]
- [Kaspersky Security for Virtualization Light Agent](#) [▢]
- [Kaspersky Embedded Systems Security for Windows](#) [▢]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [▢]

Ces composants ont une incidence sur l'exhaustivité des données de télémétrie envoyées. Si un composant est désactivé ou manquant, Kaspersky Managed Detection and Response n'envoie pas les événements de télémétrie liés à ce composant. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN arrive à expiration. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#). Si vous continuez à utiliser le fichier de configuration actuel, l'état devient **Critical** quelques jours avant la date d'expiration.

L'état **Warning** s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization Light Agent 5.2 ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) [▢], cet état n'est pas affiché.

- **Critical** (rouge)

Raisons possibles de l'état **Critical** :

- Pertes de télémétrie majeures, les données de télémétrie sont insuffisantes pour l'analyse. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

- **Surveillance du système ou Détection comportementale**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Protection contre les fichiers malicieux**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si l'un de ces composants est désactivé ou manquant, Kaspersky Managed Detection and Response interrompt l'envoi de télémétrie à partir de la ressource. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN expire bientôt ou a déjà expiré. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#).

Cet état s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization 5.2 Light Agent ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Offline (noir)**

Pas de télémétrie pendant plus de 7 jours (valeur par défaut). Dans la section **Paramètres**, vous pouvez modifier le nombre de jours d'absence de la télémétrie après lequel l'état **Offline** de la ressource s'affiche. La période peut aller de 2 à 29 jours.

Si l'état **Offline** apparaît pour vos ressources, procédez comme suit :

- Assurez-vous que les modules de l'application EPP répertoriés dans les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

L'état **Offline** ne s'applique pas aux ressources VDI (machines virtuelles temporaires).

- **Absent** (noir)

Absence de télémétrie pendant plus de 30 jours pour les ressources physiques ou pendant plus de 24 heures pour les ressources VDI (machines virtuelles temporaires).

Si l'état **Absent** s'affiche pour vos ressources :

- Assurez-vous que les modules de l'application EPP présentant les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans [la liste des ressources](#), dans [les rapports](#) et dans les données reçues via [l'interface API](#).

Vérification de l'état des ressources dans Kaspersky Security Center

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Vous pouvez vérifier l'état de vos ressources à l'aide de la fonctionnalité États des ressources MDR. Elle vous permet de vérifier quelles ressources sont actuellement protégées par Kaspersky Managed Detection and Response et lesquelles n'ont jamais envoyé de [données télémétriques](#) à Kaspersky Managed Detection and Response.

Pour les ressources sur lesquelles Kaspersky Endpoint Security for Windows 12.3 ou version ultérieure fonctionne en [configuration Endpoint Detection and Response Agent \(EDR Agent\)](#), l'état affiché dans MDR ne reflète pas l'état réel.

États des ressources qui ont envoyé des données télémétriques au moins une fois

Pour vérifier l'état des ressources, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, accédez à l'onglet **États des ressources MDR**.

2. Sélectionnez l'onglet **Tous les éléments connus**.

La liste de toutes les ressources qui ont envoyé des données télémétriques à Kaspersky Managed Detection and Response au moins une fois s'affiche.

Les détails suivants sont affichés pour chaque ressource :

État

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

L'état reflète l'état actuel de la ressource. Pour les ressources présentant l'état *OK*, *Avertissement* ou *Critique*, l'application répertorie en plus les problèmes rencontrés (le cas échéant) au cours des 72 dernières heures.

Les ressources présentent l'un des états suivants :

- **OK** (vert)

La télémétrie est envoyée, la protection est entièrement opérationnelle.

- **Warning** (jaune)

Raisons possibles de l'état **Warning** :

- Pertes de télémétrie mineures. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Les bases de données antivirus sont obsolètes depuis plus de 7 jours.
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

Pare-feu

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces réseau

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protection contre les menaces par emails et extension supplémentaire pour Microsoft Office Outlook

L'article suivant explique comment activer ou configurer ce module : [Kaspersky Endpoint Security for Windows](#) .

Protection contre les menaces Internet

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

Composant autodéfense du produit

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Ces composants ont une incidence sur l'exhaustivité des données de télémétrie envoyées. Si un composant est désactivé ou manquant, Kaspersky Managed Detection and Response n'envoie pas les événements de télémétrie liés à ce composant. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN arrive à expiration. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#). Si vous continuez à utiliser le fichier de configuration actuel, l'état devient **Critical** quelques jours avant la date d'expiration.

L'état **Warning** s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization Light Agent 5.2 ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Critical** (rouge)

Raisons possibles de l'état **Critical** :

- Pertes de télémétrie majeures, les données de télémétrie sont insuffisantes pour l'analyse. Consultez cet article : [Éviter la perte des données de télémétrie des ressources](#).
- Au moins un des modules d'application EPP suivants déployés sur la ressource est désactivé ou n'est pas installé :

- **Surveillance du système ou Détection comportementale**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Protection contre les fichiers malicieux**

Les articles suivants décrivent comment activer ou configurer ce module :

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si l'un de ces composants est désactivé ou manquant, Kaspersky Managed Detection and Response interrompt l'envoi de télémétrie à partir de la ressource. Il se peut que l'application EPP installée ne comprenne pas tous les modules de la liste.

- Le fichier de configuration KPSN expire bientôt ou a déjà expiré. L'application affiche la date d'expiration. Pensez à [mettre à jour le fichier de configuration KPSN](#).

Cet état s'applique aux ressources sur lesquelles sont installés Kaspersky Endpoint Security pour Windows 11 ou version ultérieure, Kaspersky Endpoint Security for Linux 11.2 ou version ultérieure, Kaspersky Endpoint Security for Mac 11.2 ou version ultérieure ou Kaspersky Security for Virtualization 5.2 Light Agent ou version ultérieure. Pour les ressources disposant de [Kaspersky Endpoint Security for Windows dans la configuration d'Endpoint Detection and Response Agent \(EDR Agent\)](#) , cet état n'est pas affiché.

- **Offline** (noir)

Pas de télémétrie pendant plus de 7 jours (valeur par défaut). Dans la section **Paramètres**, vous pouvez modifier le nombre de jours d'absence de la télémétrie après lequel l'état **Offline** de la ressource s'affiche. La période peut aller de 2 à 29 jours.

Si l'état **Offline** apparaît pour vos ressources, procédez comme suit :

- Assurez-vous que les modules de l'application EPP répertoriés dans les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

L'état **Offline** ne s'applique pas aux ressources VDI (machines virtuelles temporaires).

- **Absent** (noir)

Absence de télémétrie pendant plus de 30 jours pour les ressources physiques ou pendant plus de 24 heures pour les ressources VDI (machines virtuelles temporaires).

Si l'état **Absent** s'affiche pour vos ressources :

- Assurez-vous que les modules de l'application EPP présentant les états **Warning** et **Critical** sont installés et activés sur les ressources.
- Assurez-vous que Kaspersky Managed Detection and Response est [correctement déployé](#) dans votre infrastructure.

Vous pouvez masquer les ressources indiquant l'état **Absent** dans [la liste des ressources](#), dans [les rapports](#) et dans les données reçues via [l'interface API](#).

Nom de la ressource

Le nom d'un ordinateur sur le réseau.

Vous pouvez cliquer sur **Asset name** pour afficher les informations relatives à la ressource dans Kaspersky Security Center Web Console.

Identifiant de la ressource

Identifiant unique d'une ressource. L'identifiant de l'élément est généré automatiquement par Kaspersky Managed Detection and Response avant que l'élément envoie la télémétrie pour la première fois.

Domaine

Un domaine de réseau auquel appartient l'appareil.

Version du système d'exploitation

Système d'exploitation installé sur l'appareil.

Applications EPP

Application EPP installée sur l'appareil et configurée pour être utilisée avec Kaspersky Managed Detection and Response.

Interfaces

Nombre de toutes les interfaces réseau disponibles sur l'appareil.

Locataire

Le nom du [locataire](#), si la ressource appartient à l'un des locataires. Si la ressource n'appartient pas à un locataire, ce champ est vide.

Vu pour la dernière fois

Nombre de jours écoulés depuis la dernière fois que la ressource a été consultée dans la Console MDR en ligne.

Les ressources sont triées en fonction de cet attribut, par ordre décroissant.

Par défaut, les ressources qui ont été vues au cours des 30 derniers jours sont affichées. Vous pouvez étendre la période en filtrant les ressources.

3. Servez-vous des options de tri et de filtrage suivantes pour utiliser cette liste :

- Cliquez sur n'importe quel en-tête de colonne pour trier la liste en fonction des valeurs de colonne sélectionnées.
- Cliquez sur la colonne **État**, puis sélectionnez les états requis. La liste sera filtrée pour n'afficher que les ressources présentant les états sélectionnés.
- Cliquez sur **Filtre**, puis sélectionnez la période pour afficher uniquement les ressources qui ont été vues pour la dernière fois au cours de la période sélectionnée. Vous pouvez également définir une période personnalisée.
- Cliquez sur **Exporter** au-dessus de la liste des ressources pour exporter un fichier au format CSV.
- Utilisez le champ **Rechercher** pour rechercher des ressources par nom.

États des ressources qui n'ont jamais transmis de données télémétriques

Cette fonctionnalité fonctionne correctement dans Kaspersky Security Center 15.1 Windows ou versions ultérieures, Kaspersky Security Center 15.1 Linux ou versions ultérieures, et Kaspersky Next Expert View.

Pour consulter les ressources qui n'ont jamais transmis de données télémétriques, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, accédez à l'onglet **États des ressources MDR**.

2. Sélectionnez l'onglet **Impossible d'obtenir l'état des éléments**.

La Console MDR en ligne affiche la liste des ressources ajoutées à Kaspersky Security Center, mais qui n'ont jamais transmis de données télémétriques à Kaspersky Managed Detection and Response.

Les détails suivants sont affichés pour chaque appareil :

- **Nom de la ressource**

Le nom d'un ordinateur sur le réseau.

Vous pouvez cliquer sur **Asset name** pour afficher les informations relatives à la ressource dans Kaspersky Security Center Web Console.

- **Applications EPP**

Application EPP installée sur la ressource et configurée pour être utilisée avec Kaspersky Managed Detection and Response.

- **État MDR**

Le module MDR d'une application EPP installée sur une ressource peut présenter l'un des états suivants :

- *Inconnu* : contrairement aux autres états, l'état *Inconnu* n'est pas envoyé par les applications. Cette option indique que les applications ne disposent d'aucune information sur l'état du module sélectionné. Par exemple, cela peut se produire si le module sélectionné fait partie des applications installées sur l'appareil ou si l'appareil est éteint.
- *Arrêté* : le module est désactivé et ne fonctionne pas actuellement.
- *En pause* : le composant est suspendu, par exemple, après que l'utilisateur a interrompu la protection dans l'application gérée.
- *Démarrage* : le module est en cours d'initialisation.
- *En fonctionnement* : le composant est activé et fonctionne correctement.
- *Échec* : une erreur s'est produite pendant le fonctionnement du composant.
- *Non installé* : l'utilisateur n'a pas sélectionné le module en vue de l'installer lors de la configuration de l'installation personnalisée de l'application.
- *Sans licence* : la licence associée à la fonctionnalité MDR est manquante ou a expiré.

- **Serveur KSC**

Nom du Serveur d'Administration de Kaspersky Security Center qui gère la ressource sélectionnée.

- **État des composants critiques**

La liste des modules d'application EPP indispensables au fonctionnement de la solution MDR. Chaque composant indique une couleur en fonction de son état :

- La couleur jaune indique que le composant présente l'un des états suivants : **En pause**, **Démarrage**, ou **Inconnu**.
- La couleur rouge indique que le composant présente l'un des états suivants : **Arrêté**, **Échec**, **Sans licence**, ou **Non installé**.
De plus, la [fonction d'autodéfense](#) est répertoriée avec les modules d'application EPP. Si cette fonctionnalité est désactivée, un indicateur rouge s'affiche également.
- Les modules dont l'état est **En fonctionnement** ne sont pas répertoriés dans le tableau et ne présente aucun indicateur de couleur.

Pour consulter la liste complète des modules, y compris ceux qui ne sont pas indispensables au fonctionnement de la solution MDR, cliquez sur le nom de la ressource. Les modules et leurs états seront affichés dans la fenêtre des détails de la ressource.

3. Si nécessaire, vous pouvez filtrer les ressources selon l'état de la solution MDR. Pour ce faire, cliquez sur **Filtre**, puis sélectionnez les états recherchés pour la solution MDR. La Console MDR en ligne affichera uniquement les ressources pour lesquelles le module MDR présente l'un des états sélectionnés. Vous pouvez également sélectionner l'une des options suivantes :
- **Installé et activé** : la liste sera filtrée pour afficher les ressources MDR qui présentent l'un des états suivants : *Inconnu, Arrêté, En pause, Démarrage, En fonctionnement* ou *Échec*.
 - **Licence manquante ou arrivée à expiration** : la liste sera filtrée pour afficher les ressources présentant l'état *Sans licence*.
4. Si nécessaire, cliquez sur le bouton **Exporter** pour exporter la liste des ressources dans un fichier au format CSV.

Éviter la perte des données de télémétrie des ressources

Nous vous recommandons d'utiliser les dernières versions des applications et des solutions Kaspersky pour vous garantir la meilleure protection, et profiter d'un accès complet aux nouvelles fonctionnalités et aux mises à jour.

Les ressources [envoient les données de télémétrie](#) à Kaspersky Managed Detection and Response pour détecter et analyser les incidents de sécurité qui se sont déroulés sein de votre infrastructure. Si vous constatez des pertes de données télémétriques dans [l'état de la ressource](#), veuillez à suivre ces instructions :

1. Les versions recommandées des applications de Kaspersky sont installées sur vos ressources (cf. la colonne *Versions recommandées et leur durée de prise en charge* dans la section *Versions des applications de Kaspersky compatibles* de la partie [Configuration matérielle et logicielle requise](#)).
2. Le débit de votre canal réseau est conforme aux caractéristiques indiquées dans la section *Canal réseau* de la partie [Configuration matérielle et logicielle requise](#).

3. Votre [serveur proxy KSN](#) offre une capacité de traitement suffisante.

En cas de problèmes avec la capacité de débit du serveur proxy KSN, désactivez le proxy KSN dans [Stratégie KSC](#) pour forcer la connexion directe des ressources à KSN :

- a. Dans le menu principal de Kaspersky Security Center, accédez à **Appareils** → **Stratégies et profils**.
 - b. Cliquez sur la stratégie correspondante à Kaspersky Endpoint Security for Windows, Linux ou Mac. La fenêtre des propriétés de la stratégie sélectionnée s'ouvre.
 - c. Dans les propriétés de la stratégie, cliquez sur **Paramètres de l'application** → **Protection avancée contre les menaces** → **Kaspersky Security Network**.
 - d. Activez l'option **Utiliser les serveurs KSN lorsque le proxy KSN n'est pas disponible** (si cela est pertinent pour la stratégie concernée).
 - e. Cliquez sur **OK**.
4. Le proxy KSN est activé côté point de distribution dans [Kaspersky Next Expert View](#) ou Kaspersky Security Center [Web Console](#) afin d'optimiser la charge du réseau.

5. La charge de travail du Serveur d'administration de Kaspersky Security Center ne dépasse pas les [limites définies](#) [☞].
6. La version recommandée de Kaspersky Security Center indiquée dans la [Configuration matérielle et logicielle requise](#) est alors utilisée et les derniers correctifs disponibles sont installés.

Administration des incidents

Un *incident* est une activité évaluée comme critique par la technologie de détection et qui nécessite une réaction immédiate du service en ligne. Cette section fournit des informations sur l'administration des incidents existants et l'ajout de nouveaux incidents.

Vous pouvez également gérer les incidents dans la [Console MDR en ligne](#).

Pour gérer les incidents dans la Console MDR en ligne, créez un compte [Kaspersky Account](#) et demandez à votre [administrateur MDR](#) (utilisateur de la Console MDR en ligne avec le rôle **MDR Administrator**) de vous [inviter dans la Console MDR en ligne](#) à l'aide de l'adresse email que vous utilisez pour votre compte Kaspersky Account. Vous recevez alors l'e-mail d'invitation contenant le lien vers la Console MDR en ligne.

La solution MDR propose des actions de réponse que vous pouvez [traiter manuellement](#) ou [configurer pour une acceptation automatique](#).

Vous pouvez configurer des intégrations avec [KUMA](#) et [XDR](#), ce qui permet à MDR de traiter les données provenant de ces plateformes.

À propos des incidents

Qu'est-ce qu'un incident

Dans le contexte de la sécurité de l'information, un incident constitue un événement imprévu ou indésirable susceptible de perturber l'activité normale ou la sécurité de l'information.

Un événement est le signe extérieur identifié d'un état particulier d'un système, d'un service ou d'un réseau.

Dans le cadre de la solution Kaspersky MDR, le principal critère à prendre en compte lorsque l'on décide que l'activité observée constitue un incident est la capacité à mettre en œuvre des mesures efficaces visant à contrer, prévenir ou réduire les éventuels dommages découlant de Cette activité. Le tableau ci-dessous comprend des exemples de critères d'incident et de mesures possibles en fonction de la source de l'événement.

Exemples de critères de détection des incidents et de mesures d'intervention

Source de l'événement	Éventuels critères liés aux incidents	Réponses éventuelles aux incidents
Terminal	- La phase active de l'attaque qui n'a pas été automatiquement empêchée - Preuves du caractère malveillant persistent du système - Indicateurs d'incidents passés - Indicateurs d'activité d'intrusion interne côté Client (y compris les cas où l'attaque a été empêchée avec succès)	- Détection des problèmes à l'aide des solutions AO Kaspersky Lab installées sur les terminaux, et évaluation de l'efficacité de la réponse automatique (si cela est techniquement possible) - Recommandation de mesures de riposte manuelles - Demande de mesures de riposte automatiques - Recommandations pour sensibiliser les utilisateurs à la sécurité de l'information
Terminal + réseau	Événement de sécurité détecté par la technologie de détection de réseau prise en charge, qui a été confirmé sur le terminal	- Détection de problèmes au moyen des produits AO Kaspersky Lab installés sur les terminaux, ainsi que des services d'AO Kaspersky Lab pour la surveillance du trafic réseau, et évaluation de l'efficacité des mesures de réponse automatiques (dans le cas où cela est techniquement possible) - Recommandation de mesures de riposte manuelles - Demande de mesures de riposte automatiques - Informé le client

Scénarios de détection d'incidents

Scénario 1. Détection des incidents par la solution Kaspersky MDR

Dans ce scénario, un incident de sécurité de l'information est détecté grâce à la solution Kaspersky MDR. L'incident est enregistré automatiquement dans le système de suivi des incidents. Le niveau de priorité de l'incident par défaut peut être modifié ultérieurement ; il nécessite toutefois d'indiquer le motif du changement selon le tableau des niveaux de priorité d'incident (voir ci-dessous). Kaspersky MDR traite les événements enregistrés afin d'obtenir rapidement des renseignements sur l'état des infrastructures informatiques du client.

Si les causes fondamentales de l'incident sont déterminées à l'issue de l'analyse, des recommandations d'intervention sont fournies au client. Si les données ne permettent pas d'identifier la cause fondamentale de l'incident, tous les renseignements disponibles et les résultats de l'analyse sont fournis au client afin qu'il puisse mener des recherches de son côté.

Scénario 2. Détection des incidents par le client (la création d'incidents personnalisés n'est pas disponible avec certains [niveaux de licence commerciale](#))

Dans ce scénario, un incident de sécurité de l'information est détecté par le client, indépendamment de la solution Kaspersky MDR. Si l'incident doit être traité par Kaspersky MDR, le client peut enregistrer l'incident manuellement et fournir toutes les données disponibles concernant l'incident détecté à l'aide des fonctionnalités de Kaspersky MDR. Par défaut, le niveau de priorité de l'incident est défini sur **Bas**, sauf indication contraire du client lors de l'enregistrement de l'incident.

La suite du traitement de l'incident est similaire au scénario 1.

Niveaux de priorité des incidents

Niveaux de priorité des incidents et leurs descriptions

Niveau de priorité de l'incident	Description
Élevée	Incidents qui, de l'avis des experts AO Kaspersky Lab, peuvent entraîner des perturbations majeures ou un accès non autorisé aux ressources du client surveillées par Kaspersky MDR. Par exemples, l'identification de traces d'une attaque ciblée ou d'une menace inconnue nécessitant de nouvelles recherches à l'aide de méthodes de police scientifique numérique.
Moyenne	Les incidents qui, selon l'avis des experts AO de Kaspersky Lab, peuvent affecter l'efficacité ou les performances des ressources du client surveillées par Kaspersky MDR, ou peuvent entraîner une corruption unique des données.
Faible	Incidents qui, selon l'avis des experts AO de Kaspersky Lab, n'affectent pas de manière significative l'efficacité ou les performances des ressources du client surveillées par Kaspersky MDR. Par exemple, les logiciels potentiellement indésirables identifiés comme un adware ou un riskware.

Le niveau de priorité des incidents par défaut est **Faible**.

Objectifs de performance de la fourniture de la solution

Temps de réaction de la cible et valeur de la fourniture de Kaspersky MDR en fonction de la priorité de l'incident

Niveau de priorité de l'incident	Temps de réaction	Valeur cible
Élevée	1 heure	90 %
Moyenne	4 heures	90 %
Faible	24 heures	90 %

L'incident est considéré comme résolu si des recommandations sur les mesures à prendre ont été remises au client.

*Le temps de réaction est le temps qui s'écoule entre la détection de l'incident (heure de sa création) et la publication de celui-ci sur la Console MDR en ligne (heure de la mise à jour).

**Valeur cible — le pourcentage d'incidents pour lequel le temps de réaction atteint l'objectif indiqué dans le tableau.

Visualisation et recherche des incidents dans la Console MDR en ligne

Pour afficher les incidents :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre. Chaque ligne représente un incident. Vous pouvez cliquer n'importe où sur la ligne pour afficher les informations à propos de l'incident.

Les attributs d'incident suivants sont présents au-dessus de la liste :

- **ID/Created** : l'identifiant numérique de l'incident dans la Console/la date à laquelle l'incident a été créé.
- **Status** : l'un des états d'incident suivants :
 - **Open** : l'incident doit être traité par l'équipe de sécurité.
 - **Resolved** : l'équipe de sécurité a fourni une réponse à l'incident.
 - **On hold** : l'équipe de sécurité a suspendu temporairement le traitement de l'incident.
 - **Closed** : l'incident a été traité par l'équipe de sécurité et aucun travail supplémentaire n'est nécessaire.
- **Summary** : un bref commentaire à propos de l'incident dans son ensemble.
- **Tenant** : le locataire auquel un incident est attribué.
- **Updated** : la date et l'heure auxquelles l'incident a été mis à jour.

Les incidents sont triés en fonction de leur heure de mise à jour par ordre décroissant.

En haut de la liste des incidents se trouvent les boutons suivants :

- Le bouton **Columns** avec l'icône en forme de roue dentée permettant de sélectionner les colonnes à afficher dans l'onglet **History**.
- Le bouton **Filter** avec l'icône en forme d'entonnoir pour afficher les modifications liées uniquement aux cases sélectionnées.
- Le bouton **Search** avec l'icône en forme de loupe permet d'afficher les modifications liées uniquement aux mots ou aux caractères saisis.

2. Si vous souhaitez modifier le nombre d'incidents affichés par page de la liste, sélectionnez un nombre en cliquant sur l'option Nombre **entries per page** dans la partie inférieure de la page. Vous pouvez sélectionner 10, 20 ou 50 incidents par page.

Pour parcourir la liste des incidents, sélectionnez une page sous la liste. Vous pouvez utiliser les options **Précédent** et **Suivant** pour basculer entre les pages adjacentes.

Pour [filtrer les incidents](#), cliquez sur l'icône en forme d'entonnoir au-dessus de la liste.

Vous pouvez effectuer une recherche parmi les incidents en cliquant sur l'icône en forme de loupe située à côté de l'icône d'entonnoir au-dessus de la liste des incidents.

Filtrage des incidents dans la Console MDR en ligne

Pour afficher des incidents en particulier, vous pouvez créer et appliquer des filtres à la liste des incidents.

Pour créer un filtre pour la liste des incidents, procédez comme suit :

1. Dans la Console MDR en ligne, sélectionnez l'option de menu **Incidents**.

La liste des incidents s'ouvre.

2. Cliquez sur l'icône d'entonnoir située au-dessus de la liste des incidents.

Le bloc **Filter** s'affiche.

Voici les paramètres disponibles pour le filtrage :

- **Created**
Période de création de l'incident.
- **Updated**
Période de mise à jour de l'incident.
- **Priority**
Priorité de l'incident. Les priorités disponibles sont Faible, Normale et Élevée.
- **Status**
État de l'incident.
- **Resolution**
Résolution de l'incident.

- **Assets**

Les ressources disponibles.

- **Tenant**

Noms de locataires disponibles.

Vous pouvez sélectionner la valeur **Root tenant** pour afficher les incidents qui ne sont attribués à aucun de vos locataires.

Vous pouvez sélectionner la valeur **Root tenant** en plus de préciser les noms des locataires.

- **Tactics**

Tactiques MITRE disponibles pour la réponse aux incidents.

- **Response statuses**

Affiche uniquement les incidents présentant les états sélectionnés des réponses correspondantes.

3. Cliquez sur **Save** pour appliquer le filtre créé. Cliquez sur **Clear** pour supprimer le filtre créé.

Une fois que le filtre est appliqué, seuls les incidents qui répondent aux paramètres sélectionnés du filtre sont affichés dans la liste des incidents.

Création d'incidents personnalisés dans la Console MDR en ligne

La création d'incidents personnalisés n'est pas disponible avec certains [niveaux de licence commerciale](#).

Si vous considérez qu'une activité dans votre infrastructure est une menace, mais que Kaspersky Managed Detection and Response n'a pas créé d'incident automatiquement, vous pouvez ajouter un nouvel incident manuellement.

Selon les termes du contrat de niveau de service (SLA), le nombre d'incidents créés manuellement pouvant être traités par l'équipe de sécurité est limité. Des informations sur les limitations sont disponibles dans l'onglet [Utilisation de MDR de Kaspersky Security Center](#). Sur cet onglet, vous pouvez suivre l'utilisation des incidents créés manuellement pour la période en cours (par exemple, pour la semaine en cours) :

- Le nombre total d'incidents que vous pouvez créer pour la période en cours. Ces incidents doivent être traités par l'équipe de sécurité, conformément au SLA. Vous pouvez créer plus d'incidents que ceux indiqués dans l'Accord MDR, mais le respect des délais du contrat de niveau de service n'est pas garanti pour le traitement de tels incidents.
- Le nombre d'incidents restant que vous pouvez créer pour la période en cours.

Pour ajouter un nouvel incident, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre.

2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Add**.

Le bloc Nouvel incident s'affiche.

3. Remplissez les champs suivants :

- **Summary**

Un bref commentaire à propos de l'incident.

- **Description**

Informations détaillées sous forme libre sur l'incident. Le langage Markdown est pris en charge

- **Assets**

La ou les ressources compromises dans l'incident. Pour ce champ, les ressources déjà existantes dans la Console MDR en ligne et Kaspersky Security Center sont proposées.

4. Si nécessaire, remplissez le champ **Tenant**.

Pour le champ **Tenant**, les locataires déjà existants et la valeur **Racine sans locataires** sont suggérés.

5. Cliquez sur le bouton **Send**.

Le bloc Nouvel incident disparaît.

Le nouvel incident est ajouté à la liste des incidents dans la Console MDR en ligne. Vous pouvez afficher des informations détaillées sur cet incident et le traitement des réponses.

Affichage d'informations détaillées concernant les incidents dans la Console MDR en ligne

Pour afficher des informations détaillées sur les incidents, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre.

2. Cliquez sur la chaîne présentant l'incident dont vous souhaitez afficher les détails.

La page d'incident s'ouvre.

Le titre de la page contient un identifiant d'incident. Sous le titre, quatre onglets sont présents :

- **Summary**

Contient des informations générales à propos de l'incident.

- **Responses**

L'onglet Réponses contient des informations à propos des réponses à l'incident.

- **Communication**

Contient des informations à propos de la communication et des fichiers liés à l'incident.

- **History**

Contient des informations sur les modifications apportées à l'incident.

Les informations générales de l'onglet **Summary** commencent par un bref résumé de l'incident. Les informations supplémentaires indiquées dans cette section comprennent les éléments suivants :

- Priorité de l'incident
- État de l'incident
- Résolution de l'incident
- Heure de création et de mise à jour de l'incident
- Tactiques MITRE
- Techniques MITRE
- Technologie de détection

Sous le résumé de l'incident, les informations suivantes sont indiquées :

- **Affected assets**
- **Asset-based IOCs**
- **Network-based IOCs**

Les informations générales de l'onglet **Summary** se terminent par une description du client et un bouton **Close incident**.

3. Si vous savez que l'incident est un doublon ou que vous n'allez pas le résoudre, cliquez sur le bouton **Close incident**.

4. Si nécessaire, [transmettez l'incident à IR Retainer](#) afin de mener une enquête et d'éliminer les conséquences éventuelles.

5. Reportez-vous à l'onglet **Responses** pour afficher des informations sur les demandes de réponse.

Les informations de l'onglet **Responses** sont présentées sous forme de liste. Les colonnes de la liste sont les suivantes :

- **Status**
- **Asset ID**
- **Type**
- **Details**
- **Comment**
- **Changed by**
- **Update time**

6. Si vous souhaitez ajouter un commentaire à un incident, procédez comme suit :

- a. Dans l'onglet **Communication** de la page des détails de l'incident, saisissez votre commentaire dans le champ de texte.

Le langage Markdown et les fichiers joints sont pris en charge. La taille maximale du fichier est de 10 Mo

- b. Cliquez sur le bouton **Send**.

Le commentaire est ajouté à l'onglet **Communication** sur la page des détails de l'incident. Vous pouvez modifier ou supprimer votre commentaire dans les 10 minutes après l'avoir publié.

7. Reportez-vous à l'onglet **History** pour afficher les informations sur les modifications apportées à l'incident.

Sous le titre, un commutateur est présent permettant d'afficher les changements liés à ce qui suit :

- **All events**
- **Only incidents**
- **Only responses**
- **Only communication**

À côté de ce commutateur, les boutons suivants sont présents :

- Le bouton **Columns** avec l'icône en forme de roue dentée permettant de sélectionner les colonnes à afficher dans l'onglet **History**.
- Le bouton **Filter** avec l'icône en forme d'entonnoir pour afficher les modifications liées uniquement aux cases sélectionnées.
- Le bouton **Search** avec l'icône en forme de loupe permet d'afficher les modifications liées uniquement aux mots ou aux caractères saisis.

Traitement des réponses aux incidents dans la Console MDR en ligne

Vous pouvez afficher, accepter et refuser des [réponses](#) aux incidents.

Pour afficher les réponses à un incident :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre.

2. Cliquez sur la chaîne présentant l'incident dont vous souhaitez afficher les détails.

La page d'incident s'ouvre.

3. Sur la page de l'incident, cliquez sur l'onglet **Responses**.

La liste des réponses s'ouvre.

Chaque ligne représente une réponse. Les informations suivantes à propos de la réponse s'affichent :

- **Status**

L'état de la réponse.

- **Asset ID**

L'identifiant de la ressource pour la réponse à exécuter.

- **Type**

Le type de l'objet qui constitue la réponse.

- **Parameters**

Le chemin local propre au système d'exploitation pour obtenir le fichier de réponses et la taille de fichier attendue en Mo. La taille maximale du fichier est de 10 Mo

- **Comment**

Le dernier commentaire de la réponse.

- **Changed by**

Le dernier utilisateur qui a modifié la description de la réponse.

Pour afficher la description de la réponse, cliquez sur la chaîne contenant la réponse.

Pour accepter ou refuser des réponses à un incident :

1. Dans la fenêtre de la Console, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre.

2. Cliquez sur la chaîne présentant l'incident dont vous souhaitez afficher les détails.

La page d'incident s'ouvre.

3. Sur la page de l'incident, cliquez sur l'onglet **Responses**.

La liste des réponses s'ouvre.

4. Sélectionnez une réponse que vous souhaitez approuver ou refuser en cochant la case à gauche de la chaîne qui contient la réponse.

Vous pouvez également sélectionner plusieurs réponses en cochant leur case à gauche. Pour sélectionner toutes les réponses, cochez la case dans la partie gauche de l'en-tête du tableau des réponses.

5. Pour approuver ou refuser une réponse ou plusieurs réponses, sélectionnez le bouton **Accept** ou **Reject** situé sous la liste des réponses. La zone de commentaire s'affiche. Saisissez votre commentaire et cliquez sur le bouton **Send**.

Dans le volet latéral qui s'affiche, vous pouvez également cliquer sur une réponse sous l'onglet **Responses** pour en vérifier les détails et l'accepter ou le refuser. Pour refuser la réponse, vous devez saisir votre commentaire dans le champ situé sur la partie latérale.

L'état de la réponse est modifié.

Types de réponse

La solution MDR examine les incidents et crée des réponses que vous pouvez accepter ou refuser. Il s'agit de la manière par défaut de gérer les incidents dans Kaspersky Managed Detection and Response.

Cependant, vous pouvez créer manuellement des réponses [à l'aide des fonctionnalités de Kaspersky Endpoint Detection and Response Optimum](#).

Cet article décrit uniquement les types de réponses créées par la solution MDR.

Chaque réponse peut avoir un ensemble de paramètres qui sont présents dans l'onglet **Responses** d'un incident.

Les types de réponses disponibles sont les suivants :

- **Get file**

Copier un fichier de votre infrastructure vers Kaspersky SOC. Si vous acceptez cette réponse, le fichier spécifié sera copié dans Kaspersky SOC.

Notez que ce type de réponse permet d'obtenir des fichiers contenant des données personnelles et/ou confidentielles.

Les paramètres possibles sont les suivants :

- **Infected file path**

Le chemin d'accès absolu du fichier. Par exemple, C:\\file.exe.

- **Maximum file size**

La taille maximale du fichier, en Mo.

Si le fichier infecté dépasse la taille de fichier maximale spécifiée, la tentative d'acceptation de la réponse échouera, et la réponse ne sera pas effectuée, mais s'affichera dans l'onglet **History** d'un incident.

- **Isolate**

Isoler la ressource spécifiée du réseau.

Si vous devez désactiver d'urgence l'isolement du réseau, veuillez [contacter le Support technique](#) ou formuler une demande sous l'onglet **Communication** de l'incident.

Les paramètres possibles sont les suivants :

- **Password for disabling isolation**

Le mot de passe pour désactiver l'isolement. Une fois que le support technique aura reçu votre demande de désactivation de l'isolement du réseau, il vous enverra la procédure à suivre avec les détails concernant l'utilisation du mot de passe.

- **Identifiant de la tâche**

L'identifiant de tâche unique utilisé en association avec le **Password for disabling isolation** pour la désactivation manuelle de l'isolement du réseau.

- **Password details**

Vous pouvez vérifier la validité du **mot de passe** en générant une clé dérivée à partir de celui-ci et en comparant la valeur résultante avec la valeur du paramètre **Derived key**.

- **Version**

La version numérique des règles de création de mot de passe. Une version de 1 signifie que les paramètres suivants de PBKDF2 sont appliqués pour créer une clé dérivée :

- Algorithme de hachage HMACSHA256
 - 10 000 itérations
 - Longueur de clé de 32 octets

- **Salt**

Le sel au format HEX pour obtenir une clé dérivée via PBKDF2.

- **Derived key**

La clé dérivée au format HEX.

- **Exclude rules**

Tableau de règles avec les ports, les protocoles, les adresses IP et les processus personnalisés auxquels l'isolement n'est pas appliqué.

- **Direction**

Le sens du trafic. Les valeurs possibles sont : **Inbound**, **Outbound**, et **Both**.

- **Protocole**

Le numéro de protocole selon la [spécification IANA](#) ².

Les valeurs possibles sont les suivantes :

- **1** (ICMP)
 - **6** (TCP)
 - **17** (UDP)
 - **58** (IPv6-ICMP)

- **Remote port range**

La plage de ports distants spécifiés dans les champs imbriqués **From** et **To**.

- **Remote IPv4 address**

L'adresse IPv4 distante ou le masque de sous-réseau.

- **Remote IPv6 address**

L'adresse IPv6 distante ou le masque de sous-réseau.

- **Local port range**

La plage de ports locaux spécifiés dans les champs imbriqués **From** et **To**.

- **Local IPv4 address**

L'adresse IPv4 locale ou le masque de sous-réseau.

- **Local IPv6 address**

L'adresse IPv6 locale ou le masque de sous-réseau.

- **Process**

Le chemin d'accès à l'image de processus spécifié dans le champ imbriqué **Image** → **Path**.

- **Disable isolation**

Désactivation de l'isolement du réseau de la ressource spécifiée.

- **Delete registry key**

Suppression d'une clé de registre ou d'une branche de registre sur la ressource spécifiée.

Cette action est irréversible.

Les paramètres possibles sont les suivants :

- **Key**

Le chemin de la clé absolu, qui commence par HKEY_LOCAL_MACHINE ou HKEY_USERS. Par exemple, HKEY_LOCAL_MACHINE\\SYSTEM\\WebClient.

Si la clé est un lien symbolique, seule cette clé sera supprimée tandis que la clé cible du lien restera intacte.

- **Value**

La valeur clé.

Si ce paramètre n'est pas spécifié, la clé sera supprimée de manière récursive. Lors de la suppression récursive, chaque sous-clé qui est un lien symbolique sera supprimée tandis que sa clé cible restera intacte.

Si la valeur de la clé est une chaîne vide, la valeur par défaut sera supprimée.

- **Memory dump**

Création d'un vidage de mémoire et envoi à Kaspersky SOC.

Les paramètres possibles sont les suivants :

- **Dump type**

Un vidage de mémoire peut être de l'un des deux types suivants :

- **Full memory dump**

Un vidage de la mémoire entière d'une ressource.

- **Process dump**

Un vidage d'un processus spécifié.

- **Maximum file size**

La taille maximale du fichier pour le vidage au format ZIP, en Mo. La valeur par défaut est de 100 Mo.

- **Process**

L'identifiant du processus et les détails de l'image.

- **Image**

- **Path**

- Le chemin d'accès absolu du fichier. Par exemple, %systemroot%\system32\svchost.exe.

- **SHA-256**

- La somme de contrôle SHA256 au format HEX.

- **MD5**

- La somme de contrôle MD5 au format HEX.

- **Unique ID**

L'identifiant unique du processus.

- **Process count limit**

Le nombre maximal de processus pouvant être contenus dans le fichier de vidage.

- **Terminate process**

Terminez le processus sur la ressource indiquée avec Kaspersky Endpoint Security for Windows. Le processus à arrêter peut être indiqué par son nom ou son identificateur de processus (PID).

- **Run process**

Terminez le processus sur la ressource indiquée avec Kaspersky Endpoint Security for Windows.

Pour que cette réponse fonctionne, le composant PowerShell doit être installé sur la ressource. Le script à lancer et sa description sont consultables dans la [Console MDR en ligne](#).

- **Quarantine file**

Le fichier potentiellement dangereux est placé dans un stockage local spécial. Les fichiers de ce stockage sont conservés chiffrés et ne menacent pas la sécurité de l'appareil. La demande de confirmation précise la ressource, le chemin d'accès au fichier et le type de hachage du fichier (MD5 ou SHA256).

- **Restaurer le fichier depuis la quarantaine**

Restaure le fichier précédemment mis en quarantaine à son emplacement d'origine. S'il existe un fichier portant le même nom à l'emplacement d'origine, la restauration n'est pas effectuée.

- **Get artefacts**

Ce type d'action corrective peut entraîner la transmission de fichiers avec des données personnelles et confidentielles.

Disponible si vous avez configuré l'intégration à Kaspersky Anti Targeted Attack version 8.0 ou toute version ultérieure

Copie les fichiers liés aux alertes Kaspersky Anti Targeted Attack depuis l'infrastructure Kaspersky Anti Targeted Attack vers Kaspersky SOC. Les fichiers copiés sont utilisés par les analystes SOC de MDR pour enquêter sur les alertes Kaspersky Anti Targeted Attack.

Les paramètres possibles sont les suivants :

- Identifiant du nœud de la solution Kaspersky Anti Targeted Attack.
- Identifiant d'alerte Kaspersky Anti Targeted Attack.
- Catégories de fichiers à copier vers Kaspersky SOC en rapport avec les alertes :
 - Fichiers PCAP et Payload liés à une alerte IDS.
 - Rapport sur le résultat de l'analyse des fichiers dans Sandbox. Comprend des captures d'écran de l'exécution des objets, le journal des activités ainsi que d'autres données d'analyse.
 - Le fichier infecté qui a été envoyé dans Sandbox.
 - Le fichier contenant les détails de l'alerte.

Disponible si vous avez configuré l'intégration avec Kaspersky Next XDR Expert 2.1

Copie les fichiers liés aux alertes ou aux incidents à partir de Kaspersky Endpoint Detection and Response Expert, au sein de l'infrastructure Open Single Management Platform, vers Kaspersky SOC. Les fichiers copiés sont utilisés par les analystes SOC MDR pour enquêter sur les alertes et les incidents signalés par Kaspersky Endpoint Detection and Response Expert.

Les paramètres possibles sont les suivants :

- Identifiant du nœud de la solution.
- Identifiant de l'alerte ou de l'incident XDR.
- Catégories de fichiers à copier vers Kaspersky SOC qui sont liés aux alertes ou aux incidents :
 - Fichiers chargés vers l'alerte ou l'incident XDR.
 - Rapport sur le résultat de l'analyse des fichiers dans Sandbox. Comprend des captures d'écran de l'exécution des objets, le journal des activités ainsi que d'autres données d'analyse.
 - Le fichier infecté qui a été envoyé dans Sandbox.
 - Fichiers liés aux actions de réponse de l'utilisateur à l'alerte ou à l'incident :
 - Récupération de fichiers
 - Collecte de preuves numériques

- Acquisition de clés de registre
- Récupération de fichiers du service du système de fichiers NTFS
- Acquisition de vidage de mémoire de processus
- Mise en quarantaine de fichiers
- Détails sur tous les fichiers en rapport avec l'alerte.
- Noms et identifiants des fichiers copiés.

Acceptation automatique des réponses dans la Console MDR en ligne

Vous pouvez activer l'acceptation automatique des réponses proposées. Dans ce cas, les actions proposées dans les réponses, par exemple la suppression d'un fichier infecté, seront effectuées automatiquement. Lorsque cette fonction est désactivée, les [mesures proposées dans les réponses](#) doivent être acceptées ou rejetées manuellement.

Si vous utilisez des clients, vous pouvez activer l'acceptation automatique des réponses pour tous les locataires ou uniquement pour les locataires que vous sélectionnez. Si vous n'utilisez pas de locataires, activez ou désactivez cette fonctionnalité pour votre organisation actuelle.

Pour activer l'acceptation automatique des réponses, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Settings**.

2. Cliquez sur l'onglet **Incidents**.

3. Sélectionnez l'une des options suivantes :

- **Enabled for all tenants**

Lorsque cette option est sélectionnée, l'acceptation automatique des réponses est activée pour les locataires existants comme ceux créés récemment.

- **Enabled for the tenants selected below**

Sélectionnez les locataires pour lesquels vous souhaitez activer l'acceptation automatique des réponses. Pour les locataires récemment créés, l'acceptation automatique des réponses est désactivée par défaut.

4. Cliquez sur **Save**.

L'acceptation automatique des réponses est activée et les actions proposées dans les réponses seront exécutées automatiquement pour tous les locataires ou pour les locataires que vous avez sélectionnés. Vous pouvez désactiver cette option à tout moment.

Privèges d'accès pour consulter ou modifier les paramètres d'acceptation automatique

Les [rôles d'utilisateur de Kaspersky Managed Detection and Response](#) disposent des droits d'accès suivants aux paramètres d'acceptation automatique :

Fonctionnement	Administrateur MDR	Agent de sécurité principal	Responsable de la sécurité
Accédez à l'onglet Incidents .	✓	✓	—
Modifier l'option sélectionnée actuellement	✓	—	—
Afficher l'option sélectionnée actuellement	✓	✓	—
Activer l'acceptation automatique pour tous les locataires	✓	—	—
Activer l'acceptation automatique pour des locataires particuliers	✓	✓ (uniquement pour les locataires auxquels l'utilisateur a accès)	—
Afficher le paramètre d'acceptation automatique d'un locataire en particulier	✓	✓ (uniquement pour les locataires auxquels l'utilisateur a accès)	—

Acceptation automatique des réponses dans Kaspersky Security Center

Vous pouvez activer l'acceptation automatique des réponses proposées. Dans ce cas, les actions d'intervention proposées dans les réponses, par exemple la suppression d'un fichier infecté, seront effectuées automatiquement. Lorsque cette fonction est désactivée, les [mesures proposées dans les réponses](#) doivent être acceptées ou rejetées manuellement.

Si vous utilisez des clients, vous pouvez activer l'acceptation automatique des réponses pour tous les locataires ou uniquement pour les locataires que vous sélectionnez. Si vous n'utilisez pas de locataires, activez ou désactivez cette fonctionnalité pour votre organisation actuelle.

Vous pouvez modifier les paramètres d'acceptation automatique si vous disposez rôle Administrateur MDR. Les utilisateurs ayant le rôle Agent de sécurité ne sont pas autorisés à modifier les paramètres. Les utilisateurs ayant le rôle Agent de sécurité principal peuvent effectuer les opérations suivantes :

- Afficher l'option sélectionnée actuellement
- Activer ou désactiver l'acceptation automatique des réponses pour des locataires spécifiques si l'option **Autoriser la modification de l'option d'acceptation automatique des réponses pour chaque locataire** est sélectionnée

Pour configurer l'acceptation automatique des réponses, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Paramètres**.
2. Dans le groupe de paramètres **Acceptation automatique des réponses**, sélectionnez l'option désirée :

- **Désactiver l'acceptation automatique des réponses pour tous les locataires**
Sélectionnez cette option si vous souhaitez accepter ou refuser les actions d'intervention manuellement.
- **Autoriser la modification de l'option d'acceptation automatique des réponses pour tous les locataires**
Sélectionnez cette option si vous souhaitez activer l'acceptation automatique des réponses pour tous les locataires de votre organisation, y compris les locataires existants et les nouveaux.
- **Autoriser la modification de l'option d'acceptation automatique des réponses pour chaque locataire**

Sélectionnez cette option si vous souhaitez configurer individuellement l'acceptation automatique des réponses pour chaque locataire. Ensuite, cochez les cases des locataires pour lesquels vous souhaitez que les actions d'intervention soient exécutées automatiquement. Pour les locataires récemment créés, l'acceptation automatique des réponses est désactivée par défaut.

Si vous sélectionnez l'option **Tous les locataires**, l'acceptation automatique des réponses est activée par défaut pour les nouveaux locataires créés.

3. Cliquez sur **Enregistrer**.

Le bouton **Enregistrer** ne devient actif que si vous avez modifié les paramètres.

Clôture des incidents dans la Console MDR en ligne

Vous pouvez fermer un incident si vous savez qu'il s'agit d'un doublon ou que vous n'allez pas le résoudre. Dans les autres cas, vous ne devez pas fermer les incidents, car ils doivent être résolus par la solution MDR. La solution MDR résout un incident si les mesures recommandées dans le cadre de cet incident sont appliquées. Un incident résolu se ferme automatiquement au bout de 72 heures.

Pour clore un incident, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre.

2. Cliquez sur la chaîne présentant l'incident dont vous souhaitez afficher les détails.

La page d'incident s'ouvre.

3. Dans l'onglet **Summary** de la page, cliquez sur le bouton **Close incident** dans la partie inférieure de la fenêtre.

Il n'y a pas de bouton **Close incident** dans les incidents présentant l'état **Closed**.

Le bloc **Close incident** s'affiche.

4. Dans le champ **Reason why you are closing this incident**, indiquez toute information supplémentaire que vous souhaitez communiquer aux analystes SOC de Kaspersky Managed Detection and Response. Par exemple, vous pouvez expliquer pourquoi vous considérez cet incident comme une situation standard et non menaçante pour votre infrastructure. Vous pouvez laisser ce champ vide.

5. Sous le champ de commentaire, sélectionnez l'option **True positive** ou **False positive**, selon la raison de la fermeture.

Sélectionnez l'option **True positive** si Kaspersky Managed Detection and Response a détecté une menace, mais que vous ne souhaitez pas que les analystes SOC MDR enquêtent et résolvent l'incident.

Sélectionnez l'option **False positive** si Kaspersky Managed Detection and Response a considéré une activité non menaçante comme étant une menace. Kaspersky Managed Detection and Response utilise ces informations pour améliorer les algorithmes de détection automatisés.

6. Dans la partie inférieure du bloc, cliquez sur le bouton **Close**.

Le formulaire **Partagez vos commentaires** s'affiche.

7. Dans le formulaire **Partagez vos commentaires**, sélectionnez une note de 1 à 5. Vous pouvez laisser un commentaire écrit concernant la gestion de cet incident. Les commentaires sont ensuite traités par les experts de Kaspersky afin d'améliorer les performances de la solution MDR.

8. Cliquez sur **Envoyer**.

Le bloc **Close incident** disparaît.

L'incident est clos. Désormais, Kaspersky Managed Detection and Response n'effectuera aucune action en rapport avec cet incident.

Envoi d'un incident à l'équipe de réponse aux incidents pour une enquête complémentaire

Vous pouvez [envoyer un incident à l'équipe de réponse aux incidents](#) pour qu'elle mène une enquête. Ce service comprend l'ensemble complet des mesures de réponse, allant de l'analyse initiale et les premières mesures de réponse rapides à la détection de signes d'attaques supplémentaires et à la préparation d'un plan d'élimination des conséquences possibles.

Lorsque vous achetez l'abonnement au service, vous disposez d'un certain nombre d'heures d'enquête. Vous dépensez les heures d'enquête lorsque vous envoyez un incident à l'équipe de réponse aux incidents. Si vos heures d'enquête sont insuffisantes, vous pouvez toujours envoyer un incident pour enquête en sollicitant un service commercial et en créant une demande manuellement.

Vous recevez les résultats de l'enquête dans l'onglet **Communication** de l'incident.

Les utilisateurs ayant les rôles MDR Administrator ou Senior Security Officer sont autorisés à envoyer des incidents à l'équipe de réponse aux incidents.

Pour envoyer un incident à l'équipe de réponse aux incidents, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Incidents**.

La liste des incidents s'ouvre.

2. Cliquez sur la chaîne correspondant à l'incident que vous souhaitez envoyer à l'équipe de réponse aux incidents.

La page d'incident s'ouvre.

3. Sous l'onglet **Summary** de la section **Actions**, exécutez une des actions suivantes :

- Si vous disposez d'heures d'enquête, cliquez sur le bouton **Escalate incident to the IR team**, puis confirmez que vous souhaitez envoyer l'incident à l'équipe de réponse aux incidents.
- Si vous ne disposez pas d'heures d'enquête, cliquez sur le lien, puis remplissez le formulaire de demande pour acheter un service commercial.

L'incident est envoyé. Les experts de l'équipe de réponse aux incidents vous contacteront via la Console MDR en ligne dans les plus brefs délais après la réception de l'incident.

Intégration de Kaspersky Unified Monitoring and Analysis

Kaspersky Unified Monitoring and Analysis Platform (KUMA) est une solution logicielle intégrée qui combine les fonctionnalités suivantes :

- Réception, traitement et stockage des événements liés à la sécurité de l'information
- Analyse et corrélation des données entrantes
- Recherche dans les événements reçus
- Création de notifications concernant les indicateurs détectés de menaces pour la sécurité de l'information

Vous pouvez configurer l'intégration à Kaspersky Managed Detection and Response dans KUMA version 4.0 ou toute version ultérieure afin d'importer automatiquement les données KUMA dans MDR.

L'article suivant décrit comment configurer l'intégration : [Intégration à Kaspersky Managed Detection and Response](#).

Création d'incidents de Managed Detection and Response à partir d'incidents XDR

Vous pouvez créer un incident MDR à partir d'un incident XDR si l'intégration à Managed Detection and Response est activée dans Open Single Management Platform et si les alertes de l'incident XDR remplissent les conditions suivantes :

- La source de détection est le terminal.
- Au moins une ressource associée est incluse dans l'alerte.
- La technologie de détection est l'une des suivantes :
 - Règles IOA de Kaspersky
 - SB (Sandbox)
 - AM (moteur anti-malware)
 - IOC
 - YARA

Nous vous recommandons d'activer la solution MDR sur toutes les ressources gérées afin d'assurer une protection continue et d'automatiser la détection des menaces, ce qui permettra aux employés chargés de la sécurité informatique de se consacrer à des tâches qui nécessitent leur intervention.

Pour exporter un incident XDR vers MDR, procédez comme suit :

1. Dans le menu principal de l'interface de la Console OSMP, sélectionnez l'option **Surveillance** → **Incidents**.
2. Dans le tableau des incidents, cliquez sur l'identifiant de l'incident requis. La fenêtre avec les détails de l'incident s'affiche.
3. Cliquez sur l'icône représentant les trois points dans la barre d'outils et sélectionnez l'option **Créer un incident MDR**.
4. Dans le panneau **Créer un incident MDR**, indiquez le nom et la description de l'incident, puis cliquez sur **Créer**.
Si la création de l'incident a réussi, un message approprié s'affiche. Vous pouvez alors accéder à l'incident dans la Console MDR en ligne. Le lien vers l'incident est disponible dans la section **Résumé** de l'incident XDR.

Intégration de Kaspersky Digital Footprint Intelligence pour MDR

La solution MDR peut utiliser les informations d'identification compromises détectées par Kaspersky Digital Footprint Intelligence (DFI) afin d'améliorer les processus de détection, d'investigation et de recherche des menaces.

Les clients n'ont pas besoin de disposer d'une licence Kaspersky DFI active pour utiliser cette fonctionnalité. Les données de Kaspersky DFI sont disponibles dans le cadre de la fonctionnalité MDR correspondante.

La solution MDR analyse les fuites d'informations d'identification pertinentes pour l'organisation cliente ainsi que les ressources qui lui sont associées et qui sont couvertes par la surveillance MDR. L'objectif primaire concerne les fuites d'informations d'identification liées aux logiciels malveillants voleurs d'informations, qui peuvent indiquer une compromission potentielle de l'appareil d'un employé.

Les données de Kaspersky DFI sont utilisées par MDR pour les fonctionnalités suivantes :

- Enrichissement des alertes avec le contexte des fuites d'informations d'identification ;
- Corrélation des informations d'identification divulguées avec les événements de sécurité ;
- Recherche des menaces et détection d'une compromission potentielle à partir des informations d'identification.

L'intégration de Kaspersky DFI aide la solution MDR à identifier plus rapidement les comptes potentiellement compromis, à mieux hiérarchiser les incidents associés et à réduire le risque d'accès non autorisé.

Outre les fuites liées aux logiciels malveillants voleurs d'informations, Kaspersky DFI peut analyser les informations d'identification publiquement accessibles provenant de ressources tierces, sur lesquelles les informations d'identification des employés peuvent également apparaître. La portée de cette surveillance peut également s'étendre aux partenaires et à d'autres entités associées à l'organisation.

En résumé, Kaspersky DFI fournit à MDR des renseignements sur la compromission des informations d'identification, tandis que MDR exploite ces données dans les processus du SOC à des fins d'enrichissement des alertes, de corrélation et de recherche des menaces.

Utilisation des fonctionnalités de Kaspersky Endpoint Detection and Response Expert

L'intégration de Kaspersky Endpoint Detection and Response Expert au sein d'Open Single Management Platform permet de bénéficier des fonctionnalités suivantes :

- Kaspersky Endpoint Detection and Response envoie les données d'alerte à MDR, ce qui vous permet de traiter la télémétrie et les alertes Endpoint Detection and Response dans la solution MDR.
- [Possibilité de créer des incidents MDR à partir d'incidents XDR](#).
- [Type de réponse](#) Obtenir les artefacts.

Activation de l'intégration de Kaspersky Endpoint Detection and Response Expert

Le rôle Administrateur MDR est requis pour la configuration de l'intégration.

Pour activer l'intégration :

1. [Configurez le plug-in MDR](#) dans Open Single Management Platform Console.
2. Dans la section MDR de l'interface de la Console OSMP, cliquez sur l'onglet **Utilisation de MDR**.
3. Développez le groupe **fichier de configuration KPSN** pour l'intégration avec KEDR Expert.
4. Activez l'option **Accepter le contrat KPSN** et cliquez sur **Appliquer le fichier de configuration KPSN pour l'intégration avec KEDR Expert**.

L'intégration est activée.

Réponses

La solution [Kaspersky Endpoint Detection and Response Expert](#) fournit les fonctionnalités de réponse suivantes (ci-après également appelées réponses EDR) que vous pouvez exécuter et configurer manuellement.

- Isolement du réseau
- Déplacer le fichier en quarantaine
- Envoi de fichiers vers la sandbox dans le cloud
- Supprimer le fichier
- Exécuter une analyse des zones critiques
- Analyse IOC

- Prévention de l'exécution
- Lancer un processus
- Terminer le processus
- Obtenir le fichier

Pour en savoir plus sur ces réponses EDR, consultez l' [aide en ligne de Kaspersky Endpoint Detection and Response Expert](#).

Les réponses EDR décrites dans cette section sont disponibles pour les ressources disposant de Kaspersky Endpoint Security for Windows 11.7 ou version ultérieure. Si vous utilisez Kaspersky Endpoint Security for Windows 11.6 ou une version antérieure sur vos ressources, Kaspersky Endpoint Agent doit être installé sur ces ressources pour que les réponses EDR soient traitées.

Pour gérer les actions des réponses aux alertes EDR, dans [Kaspersky Security Center](#) ² accédez à la section **Suivi et rapports** → **Alertes**.

Gestion des locataires

La multilocation est un mécanisme qui vous permet de devenir un fournisseur Kaspersky Managed Detection and Response pour d'autres organisations. Une fois que vous avez un compte MDR, vous pouvez créer des [locataires](#) dans votre compte MDR.

Vous pouvez créer jusqu'à 100 locataires dans votre organisation.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Si votre organisation dispose de plusieurs licences, vous ne pouvez [gérer les locataires que dans Kaspersky Security Center](#).

Pour devenir un fournisseur MDR, vous devez avoir accès à l'infrastructure de votre locataire pour pouvoir effectuer des scénarios de déploiement.

Tous les locataires sont indépendants et isolés, ce qui signifie qu'aucune donnée d'un locataire n'est accessible aux autres locataires.

Les ressources avec Kaspersky Embedded Systems Security for Windows et Kaspersky Embedded Systems Security for Linux peuvent uniquement être attribuées au locataire racine.

Seuls les utilisateurs dotés du rôle [Administrateur MDR](#) peuvent ajouter, modifier et supprimer des clients dans la Console MDR en ligne.

Gestion des locataires dans Kaspersky Security Center

Cette section fournit des informations sur la gestion des locataires existants et l'ajout de nouveaux locataires dans Kaspersky Security Center.

Affichage des clients dans Kaspersky Security Center

Vous pouvez afficher les locataires disponibles en utilisant la liste des locataires.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Pour afficher les locataires :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Locataires**.

La liste des **Locataires** s'affiche. Chaque ligne représente un locataire. Vous pouvez cliquer sur le nom du locataire pour afficher ses informations.

2. Les attributs de locataire suivants sont présents au-dessus de la liste :

Nom

Nom arbitraire et lisible du locataire que vous indiquez lors de la création du locataire. Le nom du locataire peut contenir des lettres latines, des chiffres et des caractères spéciaux. Il ne peut pas comporter plus de 100 caractères. Les locataires ne peuvent pas être renommés.

État

L'un des états du locataire suivants :

- **Actif**

Un locataire peut utiliser Kaspersky Managed Detection and Response.

- **Inactif**

Un locataire ne peut pas utiliser Kaspersky Managed Detection and Response.

Vous pouvez définir manuellement l'état inactif sur la carte de locataire. De plus, l'état inactif est défini automatiquement à la fin de la vie du locataire.

Ressources/Limite

Nombre de ressources attribuées à un locataire/Limite de ressources.

La limite de ressources est spécifiée lors de la création de locataires supplémentaires et est fournie à titre d'information uniquement. Le dépassement est autorisé et n'influence pas le fonctionnement de la solution MDR.

Description

Informations de forme libre que vous saisissez lors de la création ou de la modification du locataire. Vous pouvez préciser l'objectif du locataire ou le nombre prévu de ressources. La description peut contenir des lettres latines, des chiffres et des caractères spéciaux. Elle ne peut pas comporter plus de 2 000 caractères.

Date de création

Date de création du locataire.

Date d'expiration

Date à laquelle la durée de vie du locataire expire.

Les locataires sont triés en fonction de leur date d'expiration par ordre décroissant.

Vous pouvez également [afficher les locataires dans la Console MDR en ligne](#).

Affichage des paramètres des locataires dans Kaspersky Security Center

Vous pouvez afficher les paramètres de chaque locataire de votre compte.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Pour afficher les paramètres du locataire, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Locataires**.

La liste des **Locataires** s'affiche. Chaque ligne représente un locataire. Vous pouvez cliquer sur le nom du locataire pour afficher ses informations.

2. Cliquez sur la ligne présentant le locataire dont vous souhaitez afficher les détails.

Le bloc **Paramètres du locataire** apparaît.

Le paramètre commence par le commutateur **Actif** indiquant si un locataire est actif ou non. Si nécessaire, vous pouvez basculer le commutateur en position **Actif**. Ci-dessous, les champs suivants sont présents :

Nom

Nom arbitraire et lisible du locataire que vous indiquez lors de la création du locataire. Le nom du locataire peut contenir des lettres latines, des chiffres et des caractères spéciaux. Il ne peut pas comporter plus de 100 caractères. Les locataires ne peuvent pas être renommés.

Identifiant

Un identifiant unique de locataire généré automatiquement.

Description

Informations de forme libre que vous saisissez lors de la création ou de la modification du locataire. Vous pouvez préciser l'objectif du locataire ou le nombre prévu de ressources. La description peut contenir des lettres latines, des chiffres et des caractères spéciaux. Elle ne peut pas comporter plus de 2 000 caractères.

Locataires affectés

Le nombre de ressources attribuées au locataire.

Limite de ressources

Le nombre de ressources qu'il est prévu d'associer au locataire. Il est permis de dépasser cette limite, ce qui n'affecte en rien le fonctionnement de la solution MDR.

Fichiers de configuration du locataire

Cette section affiche des informations à propos du [fichier de configuration MDR](#) pour le locataire :

- **Licence** : la [licence](#) qui correspond au locataire.
- **Date d'expiration** : durée de vie du locataire. Vous pouvez préciser la date d'expiration manuellement lors de la création du locataire. La date d'expiration de ce locataire ne peut pas être égale ni postérieure au dernier jour de la durée de votre licence MDR.
- **Action** : Vous pouvez cliquer sur le lien **Télécharger le fichier de configuration** pour télécharger l'archive ZIP qui contient le fichier de configuration du Conteneur MDR.

Cliquez sur le bouton **X** pour supprimer un fichier de configuration. Vous ne pouvez supprimer un fichier de configuration que si un autre fichier de configuration est ajouté au locataire.

Cliquez sur le bouton **Ajouter** pour ajouter un nouveau fichier de configuration. Précisez la licence et la date d'expiration.

3. Dans la partie inférieure du bloc **Paramètres du locataire**, cliquez sur le bouton **Fermer** pour fermer le bloc.

Vous pouvez également afficher les [paramètres du locataire dans la Console MDR en ligne](#).

Modification des paramètres des locataires dans Kaspersky Security Center

Vous pouvez modifier les paramètres de chaque locataire de votre compte.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Pour modifier les paramètres du locataire, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Locataires**.

La liste des **Locataires** s'affiche. Chaque ligne représente un locataire. Vous pouvez cliquer sur le nom du locataire pour afficher ses informations.

2. Cliquez sur la ligne présentant le locataire dont vous souhaitez modifier les détails.

Le bloc **Paramètres du locataire** apparaît. Ici, vous pouvez effectuer les actions suivantes :

- Activer ou désactiver le locataire en activant le bouton à bascule **Actif**.
- Modifier la valeur du champ **Description**.
- Supprimer un fichier de configuration en cliquant sur le bouton **X**. Vous ne pouvez supprimer un fichier de configuration que si un autre fichier de configuration est ajouté au locataire.
- Ajout d'un nouveau fichier de configuration en cliquant sur le bouton **Save**. Précisez la licence et la date d'expiration.

3. Dans la partie inférieure du bloc **Paramètres du locataire**, cliquez sur le bouton **Save**.

- Le bloc **Paramètres du locataire** disparaît. Après que vous avez cliqué sur le bouton **Save**, Kaspersky Managed Detection and Response génère le nouveau fichier de configuration MDR conforme aux paramètres du locataire mis à jour. Vous pouvez cliquer sur le lien **Télécharger le fichier de configuration** pour télécharger l'archive ZIP contenant le fichier de configuration MDR.

Les paramètres du locataire sont modifiés. Les paramètres mis à jour sont appliqués aux ressources des groupes d'administration sélectionnés.

Vous pouvez également modifier les [paramètres du locataire dans la Console MDR en ligne](#).

Ajout de nouveaux locataires dans Kaspersky Security Center

Si vous souhaitez devenir un fournisseur Kaspersky Managed Detection and Response pour une autre organisation, vous devez ajouter un nouveau locataire à votre compte.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Pour ajouter un nouveau locataire, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Locataires**.

La liste des **Locataires** s'affiche.

2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **+ Ajouter un locataire**.

Le bloc **Paramètres du locataire** apparaît.

3. Si nécessaire, activez le commutateur **Actif**.

Le commutateur **Actif** est activé par défaut.

4. Remplissez les champs suivants :

Nom

Nom arbitraire et lisible du locataire que vous indiquez lors de la création du locataire. Le nom du locataire peut contenir des lettres latines, des chiffres et des caractères spéciaux. Il ne peut pas comporter plus de 100 caractères. Les locataires ne peuvent pas être renommés.

Description

Informations de forme libre que vous saisissez lors de la création ou de la modification du locataire. Vous pouvez préciser l'objectif du locataire ou le nombre prévu de ressources. La description peut contenir des lettres latines, des chiffres et des caractères spéciaux. Elle ne peut pas comporter plus de 2 000 caractères.

Fichiers de configuration du locataire

Cette section affiche des informations à propos du [fichier de configuration MDR](#) pour le locataire :

- **Licence** : la [licence](#) qui correspond au locataire.
- **Date d'expiration** : durée de vie du locataire. Vous pouvez préciser la date d'expiration manuellement lors de la création du locataire. La date d'expiration de ce locataire ne peut pas être égale ni postérieure au dernier jour de la durée de votre licence MDR.
- **Action** : Vous pouvez cliquer sur le lien **Télécharger le fichier de configuration** pour télécharger l'archive ZIP qui contient le fichier de configuration du Conteneur MDR.

Cliquez sur le bouton **X** pour supprimer un fichier de configuration. Vous ne pouvez supprimer un fichier de configuration que si un autre fichier de configuration est ajouté au locataire.

Cliquez sur le bouton **Ajouter** pour ajouter un nouveau fichier de configuration. Précisez la licence et la date d'expiration.

Limite de ressources

Le nombre de ressources qu'il est prévu d'associer au locataire. Il est permis de dépasser cette limite, ce qui n'affecte en rien le fonctionnement de la solution MDR.

5. Dans la partie inférieure du bloc **Paramètres du locataire**, cliquez sur le bouton **Enregistrer**.

Le bloc **Paramètres du locataire** disparaît. Après que vous avez cliqué sur le bouton **Enregistrer**, Kaspersky Managed Detection and Response génère [le fichier de configuration MDR](#) pour le nouveau locataire. Vous pouvez cliquer sur le lien **Télécharger le fichier de configuration** pour télécharger l'archive ZIP contenant le fichier de configuration MDR.

Le nouveau locataire est ajouté.

Vous pouvez également [ajouter de nouveaux locataires dans la Console MDR en ligne](#).

Suppression des locataires dans Kaspersky Security Center

Lorsque vous supprimez un locataire qui contient des ressources, toutes ses ressources sont déconnectées de la solution MDR. Pour continuer à gérer les ressources du locataire, vous pouvez [les déplacer vers le locataire racine ou un nouveau locataire](#) avant de supprimer le locataire.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Pour supprimer un locataire :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **Locataires**.

La liste des **Locataires** s'affiche.

2. Dans la liste des **Locataires**, pointez sur le locataire que vous souhaitez supprimer, puis cliquez sur l'icône de la corbeille () dans la colonne **Actions**.

3. Confirmez la suppression.

Le locataire sélectionné est supprimé.

Vous pouvez également [supprimer des locataires dans la Console MDR en ligne](#).

Déplacement de ressources entre locataires

Lorsque vous supprimez un locataire qui contient des ressources, toutes ses ressources cessent d'envoyer des données télémétriques à la solution MDR. Avant de supprimer un locataire, il faut déplacer toutes ses ressources vers le locataire racine ou vers un nouveau locataire.

Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, votre compte doit comporter un rôle disposant des [droits d'accès](#) suivants : **Accès aux incidents** et **Gestion des locataires**, ainsi que de la possibilité d'afficher, d'ajouter, de modifier et de supprimer des locataires dans la section **MDR** de Kaspersky Security Center.

Pour déplacer des ressources vers un nouveau locataire, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, [créez un nouveau locataire](#). Plus tard, vous ajouterez des ressources à ce client.

Lorsque vous créez un nouveau locataire, vous téléchargez un fichier de configuration MDR.

2. Dans Kaspersky Security Center Web Console, [créez un nouveau groupe d'administration](#).
3. [Ajouter les ressources](#) que vous souhaitez déplacer vers un nouveau locataire vers le nouveau groupe d'administration.
4. [Créer une nouvelle politique](#) pour Kaspersky Endpoint Agent ou une application EPP pour le groupe d'administration créé.
5. Appliquez le fichier de configuration MDR à la politique créée.

Pour plus de détails sur les différents scénarios de déploiement, consultez [Déploiement de Kaspersky Managed Detection and Response](#).

Une fois la politique appliquée aux ressources du groupe d'administration, les ressources sont déplacées du locataire racine vers le locataire nouvellement créé.

Pour déplacer des ressources vers le locataire racine, procédez comme suit :

1. Téléchargez le fichier de configuration MDR du client racine :
 - Dans la console MDR en ligne (<https://mdr.kaspersky.com/guide>), accédez à la page **Getting Started** et cliquez sur le lien **Fichier de configuration MDR**.
 - Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, accédez à **MDR > Getting Started** et cliquez sur le lien **Télécharger**.
2. Dans Kaspersky Security Center Web Console, [créez un nouveau groupe d'administration](#).
3. [Ajoutez les ressources](#) que vous souhaitez déplacer vers le locataire racine au nouveau groupe d'administration.

4. [Créer une nouvelle politique](#) pour Kaspersky Endpoint Agent ou une application EPP pour le groupe d'administration créé.

5. Appliquez le fichier de configuration MDR à la politique créée.

Une fois la politique appliquée aux ressources du groupe d'administration, les ressources sont déplacées vers le locataire racine.

Gestion des locataires dans la Console MDR en ligne

Cette section fournit des informations à propos de la gestion des locataires dans la Console MDR en ligne.

Affichage des locataires dans la Console MDR en ligne

Pour afficher les locataires :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Settings**.

2. Cliquez sur l'onglet **Tenants**.

La liste des **Tenants** s'affiche. Chaque ligne représente un locataire. Vous pouvez cliquer n'importe où sur la ligne pour afficher les informations à propos du locataire.

3. Les attributs de locataire suivants sont présents au-dessus de la liste :

Name

Nom arbitraire et lisible du locataire que vous indiquez lors de la création du locataire. Le nom du locataire peut contenir des lettres latines, des chiffres et des caractères spéciaux. Il ne peut pas comporter plus de 100 caractères. Les locataires ne peuvent pas être renommés.

Status

L'un des états du locataire suivants :

- **Actif**

Un locataire peut utiliser Kaspersky Managed Detection and Response.

- **Inactif**

Un locataire ne peut pas utiliser Kaspersky Managed Detection and Response.

Vous pouvez définir manuellement l'état inactif sur la carte de locataire. De plus, l'état inactif est défini automatiquement à la fin de la vie du locataire.

Assets / limit

Nombre de ressources attribuées à un locataire/Limite de ressources.

La limite de ressources est spécifiée lors de la création de locataires supplémentaires et est fournie à titre d'information uniquement. Le dépassement est autorisé et n'influence pas le fonctionnement de la solution MDR.

Description

Informations de forme libre que vous saisissez lors de la création ou de la modification du locataire. Vous pouvez préciser l'objectif du locataire ou le nombre prévu de ressources. La description peut contenir des lettres latines, des chiffres et des caractères spéciaux. Elle ne peut pas comporter plus de 2 000 caractères.

Created on

Date de création du locataire.

Expiration date

Date à laquelle la durée de vie du locataire expire.

Les locataires sont triés en fonction de leur date d'expiration par ordre décroissant.

Actions

Affiche l'icône de corbeille (🗑️) au survol pour les locataires non racine. Pour supprimer le locataire, cliquez sur l'icône de corbeille et confirmez la suppression.

Affichage des paramètres des locataires dans la Console MDR en ligne

Pour afficher les paramètres du locataire, procédez comme suit :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Settings**.

2. Cliquez sur l'onglet **Tenants**.

La liste des **Tenants** s'affiche. Chaque ligne représente un locataire. Vous pouvez cliquer n'importe où sur la ligne pour afficher les informations à propos du locataire.

3. Cliquez sur la ligne présentant le locataire dont vous souhaitez afficher les détails.

Le bloc **Tenant settings** apparaît.

Le paramètre commence par le commutateur **Active** indiquant si un locataire est actif ou non. Vous pouvez actionner le commutateur **Active** pour désactiver le locataire.

Ci-dessous, les champs suivants sont présents :

Tenant name

Nom arbitraire et lisible du locataire que vous indiquez lors de la création du locataire. Le nom du locataire peut contenir des lettres latines, des chiffres et des caractères spéciaux. Il ne peut pas comporter plus de 100 caractères. Les locataires ne peuvent pas être renommés.

Description

Informations de forme libre que vous saisissez lors de la création ou de la modification du locataire. Vous pouvez préciser l'objectif du locataire ou le nombre prévu de ressources. La description peut contenir des lettres latines, des chiffres et des caractères spéciaux. Elle ne peut pas comporter plus de 2 000 caractères.

Assets / limit

Le nombre de ressources qu'il est prévu d'associer au locataire. Il est permis de dépasser cette limite, ce qui n'affecte en rien le fonctionnement de la solution MDR.

Configuration file lifetime

Date à laquelle le fichier de configuration du locataire expire.

Ce champ ne s'affiche pas pour le locataire racine.

Dans la partie inférieure du bloc, un bouton est présent permettant de télécharger le [fichier de configuration MDR](#) pour le déploiement du locataire.

4. Dans la partie inférieure du bloc **Tenant settings**, cliquez sur le bouton **Cancel** pour fermer le bloc.

Modification des paramètres des locataires dans la Console MDR en ligne

La possibilité d'ajouter, de modifier et de supprimer des locataires n'est disponible que pour l'utilisateur auquel le rôle [Administrateur MDR](#) est attribué.

Pour modifier les paramètres du locataire, procédez comme suit :

1. Ouvrez la Console MDR en ligne.

2. Dans la section **Settings** de la Console MDR en ligne, cliquez sur l'onglet **Tenants**.

La liste des **Tenants** s'affiche. Chaque ligne représente un locataire. Vous pouvez cliquer n'importe où sur la ligne pour afficher les informations à propos du locataire.

3. Cliquez sur la ligne présentant le locataire dont vous souhaitez modifier les détails.

Le bloc **Tenant settings** apparaît.

4. Si nécessaire, activez le commutateur **Active**.

5. Si nécessaire, modifiez les valeurs des champs.

6. Dans la partie inférieure du bloc **Tenant settings**, cliquez sur le bouton **Save**.

Le bloc **Tenant settings** disparaît. Après que vous avez cliqué sur le bouton **Save**, Kaspersky Managed Detection and Response génère le nouveau fichier de configuration MDR conforme aux paramètres du locataire mis à jour.

7. Dans la liste **Tenants**, cliquez sur la ligne avec le locataire modifié.

Le bloc **Tenant settings** apparaît. Dans la partie inférieure du bloc, un bouton est présent permettant de télécharger le [fichier de configuration MDR](#) pour le déploiement du locataire.

8. Dans la partie inférieure du bloc **Tenant settings**, cliquez sur le bouton **Cancel** pour fermer le bloc.

Les paramètres du locataire sont modifiés. Maintenant, vous devez déployer le nouveau fichier de configuration MDR sur les ressources du locataire pour appliquer les paramètres modifiés.

Ajout de nouveaux locataires dans la Console MDR en ligne

La possibilité d'ajouter, de modifier et de supprimer des locataires n'est disponible que pour l'utilisateur auquel le rôle [Administrateur MDR](#) est attribué.

Pour ajouter un nouveau locataire, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Settings**.

2. Cliquez sur l'onglet **Tenants**.

La liste des **Tenants** s'affiche.

3. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Add**.

Le bloc **Tenant settings** apparaît.

4. Si nécessaire, activez le commutateur **Active**.

Le commutateur **Active** est activé par défaut.

5. Remplissez les champs suivants :

Tenant name

Nom arbitraire et lisible du locataire que vous indiquez lors de la création du locataire. Le nom du locataire peut contenir des lettres latines, des chiffres et des caractères spéciaux. Il ne peut pas comporter plus de 100 caractères. Les locataires ne peuvent pas être renommés.

Description

Informations de forme libre que vous saisissez lors de la création ou de la modification du locataire. Vous pouvez préciser l'objectif du locataire ou le nombre prévu de ressources. La description peut contenir des lettres latines, des chiffres et des caractères spéciaux. Elle ne peut pas comporter plus de 2 000 caractères.

Assets / limit

Le nombre de ressources qu'il est prévu d'associer au locataire. Il est permis de dépasser cette limite, ce qui n'affecte en rien le fonctionnement de la solution MDR.

Configuration file lifetime

Date à laquelle le fichier de configuration du locataire expire.

Ce champ ne s'affiche pas pour le locataire racine.

6. Dans la partie inférieure du bloc **Tenant settings**, cliquez sur le bouton **Save**.

Le bloc **Tenant settings** disparaît. Après que vous avez cliqué sur le bouton **Save**, Kaspersky Managed Detection and Response génère [le fichier de configuration MDR](#) pour le nouveau locataire.

7. Dans la liste **Tenants**, cliquez sur la ligne avec le nouveau locataire.

Le bloc **Tenant settings** apparaît. Vous pouvez télécharger ici le [fichier de configuration MDR](#) pour le déploiement du locataire.

8. Cliquez sur le bouton **Configuration archive** pour télécharger le nouveau fichier de configuration MDR.

9. Dans la partie inférieure du bloc **Tenant settings**, cliquez sur le bouton **Cancel** pour fermer le bloc.

Le nouveau locataire est ajouté. Maintenant, vous pouvez déployer le fichier de configuration MDR téléchargé sur les ressources du locataire.

Veuillez noter que les locataires créés dans la Console MDR en ligne ne sont pas disponibles dans la section **MDR** de Kaspersky Security Center. Veuillez utiliser la Console MDR en ligne pour travailler avec ces locataires.

Suppression des locataires dans la Console MDR en ligne

Lorsque vous supprimez un locataire qui contient des ressources, toutes ses ressources sont déconnectées de la solution MDR. Les incidents attribués à un locataire supprimé ne sont plus disponibles. Cette action est irréversible. Avant de supprimer un locataire, il faut [déplacer toutes ses ressources vers le locataire racine ou vers un nouveau locataire](#).

La possibilité d'ajouter, de modifier et de supprimer des locataires n'est disponible que pour l'utilisateur auquel le rôle [Administrateur MDR](#) est attribué.

Pour supprimer un locataire :

1. Dans la Console MDR en ligne, accédez à l'option du menu **Settings**.
2. Cliquez sur l'onglet **Tenants**.
La liste des **Tenants** s'affiche.
3. Dans la liste des locataires, passez le curseur de la souris sur le locataire que vous souhaitez supprimer, puis cliquez sur le bouton **Delete tenant** avec l'icône de la corbeille sur la droite.
La fenêtre **Confirm tenant deletion** s'affiche.
4. Cliquez sur le bouton **Delete** pour supprimer le locataire.

Veuillez noter que les locataires créés dans la Console MDR ne sont pas disponibles dans la section **MDR** de Kaspersky Security Center. Veuillez utiliser la Console MDR en ligne pour travailler avec ces locataires.

Gestion de la solution via l'API REST

Cette fonctionnalité est disponible dans MDR Expert, MDR Advanced (disponible dans certaines régions uniquement) et MDR Prime (disponible dans certaines régions uniquement). Découvrez la comparaison des solutions de licence dans [cette section](#).

Pour avoir accès à l'API REST dans Kaspersky Security Center, votre compte dans Kaspersky Security Center Web Console doit disposer des droits d'accès suivants : Accès aux incidents et Accès à l'API REST.

Pour certains [niveaux de licence commerciale](#), il sera possible de générer un jeton d'actualisation dans la Console MDR en ligne uniquement pour [configurer le plug-in MDR](#), sans accéder à l'API REST dans Kaspersky Security Center.

Kaspersky Managed Detection and Response vous permet d'obtenir, de créer et de mettre à jour par programmation des entités MDR via l'API REST. L'API REST fonctionne sur le protocole HTTP et se compose d'un ensemble de méthodes de requête/réponse. Autrement dit, vous pouvez gérer Kaspersky Managed Detection and Response via une solution tierce, et non via la Console MDR en ligne.

Pour commencer à utiliser l'API REST, vous devez [créer un jeton d'actualisation](#) et [un jeton d'accès](#).

[OUVRIR LA RÉFÉRENCE DE L'API REST](#) 

Scénario : effectuer une autorisation basée sur des jetons

Ce scénario explique comment effectuer une autorisation basée sur des jetons afin d'utiliser l'API REST.

Conditions préalables

Assurez-vous que vous disposez d'un compte MDR avec l'un des rôles suivants :

- Le [rôle](#) Administrateur MDR
- Un rôle personnalisé disposant des [droits d'accès](#) suivants (applicable uniquement pour Kaspersky Security Center) :
 - Accès aux incidents
 - Accès à l'API REST

Étapes

L'autorisation basée sur des jetons se déroule par étapes :

1 Création d'un jeton d'actualisation dans la Console MDR en ligne

Vous avez besoin d'un [jeton d'actualisation](#) pour créer un jeton d'accès. Un jeton d'actualisation est valide pendant 24 heures. Vous ne pouvez utiliser un jeton d'actualisation qu'une seule fois.

2 Création d'un jeton d'accès via l'API REST

Vous avez besoin d'un [jeton d'accès](#) pour utiliser l'API REST. Un jeton d'accès est valable 1 heure. Vous pouvez utiliser un jeton d'accès plusieurs fois au cours de sa durée de vie.

Lorsque vous créez un jeton d'accès, l'API REST génère un nouveau jeton d'actualisation et l'inclut dans la réponse. Lorsque le jeton d'accès expire, vous pouvez créer un nouveau jeton d'accès à l'aide du jeton d'actualisation généré par l'API la plus récente.

Un jeton d'actualisation généré par l'API est valide pendant 7 jours.

Résultats

À la fin de ce scénario, vous pouvez [commencer à travailler avec l'API REST](#) en envoyant des demandes avec le jeton d'accès.

Création d'une connexion API dans Kaspersky Security Center

Lorsque vous créez une nouvelle connexion API, un jeton d'actualisation est généré. Un *jeton d'actualisation* est une séquence unique de lettres, de chiffres et de symboles. Une fois créé, un jeton d'actualisation vous permet de créer un jeton d'accès.

Pour créer une connexion API :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **API**.

La liste des **API** s'affiche.

2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Ajouter une connexion**.

Le bloc **Ajouter une nouvelle connexion API** apparaît.

3. Spécifiez les paramètres suivants :

- **Nom de la connexion**

Un nom de connexion peut contenir des lettres latines, des chiffres et des caractères spéciaux. Le nom de connexion est spécifié en tant que `author_name` dans les réponses de l'API REST et affiché en tant qu'auteur de commentaire dans l'onglet **Communication** d'un incident.

- **Droits d'accès**

Sélectionnez les droits d'accès à accorder pour effectuer des actions via l'API HTTP :

- **Accès complet + API et locataires**

Droits d'accès du rôle Administrateur MDR. Un Administrateur MDR est un superutilisateur qui a accès à l'ensemble des fonctions de Kaspersky Managed Detection and Response accordées par la licence. L'administrateur MDR peut accorder l'accès aux sources de données client à d'autres utilisateurs. Lorsque vous activez Kaspersky Managed Detection and Response, vous devenez automatiquement l'administrateur MDR, c'est pourquoi, dans le cadre du processus d'activation, nous vous recommandons d'utiliser une adresse e-mail d'entreprise plutôt qu'une adresse e-mail personnelle. La création d'un compte d'administrateur MDR avec une adresse e-mail personnelle peut poser des risques de sécurité tels que le vol du compte d'administrateur MDR.

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	✓	—
Programmation du résumé des incidents	✓	—
Accès à l'API REST	✓	—

- **Accès aux incidents, gestion des réponses et paramètres d'auto-acceptation**

Droits d'accès du rôle d'agent de sécurité principal. Un agent de sécurité principal est un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. L'Agent de sécurité principal a le droit d'accepter et de refuser des [réponses](#).

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

- **Accès aux incidents**

Droits d'accès du rôle d'agent de sécurité. Un agent de sécurité est un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. Le responsable de la sécurité ne peut ni accepter ni refuser des [réponses](#).

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	—	✓
Gestion des réponses	—	✓
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

- **Locataire**

Si nécessaire, sélectionnez la valeur (ou les valeurs) dans la liste déroulante **Locataire**.

L'utilisateur peut afficher uniquement les ressources et les incidents liés aux locataires indiqués.

4. Cliquez sur le bouton **Générer**.

Le champ du **Jeton JWT** s'affiche.

5. Cliquez sur le bouton **Fermer**.

La nouvelle connexion API apparaît dans la liste des **API**. Maintenant, vous pouvez utiliser ce jeton d'actualisation pour [créer un jeton d'accès](#).

Vous pouvez également [créer des connexions API dans la Console MDR en ligne](#).

Création d'une connexion API dans la Console MDR en ligne

Un *jeton d'actualisation* est une séquence unique de lettres, de chiffres et de symboles. Une fois créé, un jeton d'actualisation vous permet de créer un jeton d'accès.

Pour créer un jeton d'actualisation, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Settings**.

2. Cliquez sur l'onglet **API**.

La liste **All tokens** s'affiche.

3. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Add**.

Un bloc **Generate token** s'affiche.

4. Spécifiez les paramètres suivants :

- **Connection name**

Le nom d'un jeton.

Le nom d'un jeton peut contenir des lettres latines, des chiffres et des caractères spéciaux. Le nom d'un jeton est spécifié en tant que `author_name` dans les réponses de l'API REST et affiché en tant qu'auteur de commentaire dans l'onglet **Communication** d'un incident.

Pour certains [niveaux de licence commerciale](#), il s'agit du seul champ disponible lors de la création d'un jeton d'actualisation.

- **User role**

Le rôle d'utilisateur pour spécifier les autorisations qui seront accordées pour effectuer des actions via l'API HTTP.

Les rôles d'utilisateur suivants sont disponibles :

- **MDR Administrator**

Le superutilisateur qui a accès à l'ensemble des fonctions de Kaspersky Managed Detection and Response accordées par la licence. L'administrateur MDR peut accorder l'accès aux sources de données client à d'autres utilisateurs. Lorsque vous activez Kaspersky Managed Detection and Response, vous devenez automatiquement l'administrateur MDR, c'est pourquoi, dans le cadre du processus d'activation, nous vous recommandons d'utiliser une adresse e-mail d'entreprise plutôt qu'une adresse e-mail personnelle. La création d'un compte d'administrateur MDR avec une adresse e-mail personnelle peut poser des risques de sécurité tels que le vol du compte d'administrateur MDR.

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	✓	—
Programmation du résumé des incidents	✓	—
Accès à l'API REST	✓	—

- **Senior Security Officer**

Un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. L'Agent de sécurité principal a le droit d'accepter et de refuser des [réponses](#).

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	✓	—
Gestion des réponses	✓	—
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

- **Security Officer**

Un employé qui a accès aux fonctions Kaspersky Managed Detection and Response accordées par la licence, mais qui n'a pas accès à l'API REST. Le responsable de la sécurité ne peut ni accepter ni refuser des [réponses](#).

Dans Kaspersky Security Center, ce rôle correspond aux droits d'accès suivants :

Domaine fonctionnel	Autoriser	Refuser
Accès aux incidents	✓	—
Paramètres d'auto-acceptation	—	✓
Gestion des réponses	—	✓
Gestion des locataires	—	✓
Programmation du résumé des incidents	—	✓
Accès à l'API REST	—	✓

- **Tenant**

Si nécessaire, sélectionnez la valeur (ou les valeurs) dans la liste déroulante **Tenant**.

Les locataires déjà existants dans la Console et la valeur **Root tenant** sont suggérés.

L'utilisateur peut afficher uniquement les ressources et les incidents liés aux locataires indiqués. Si vous avez des ressources et des incidents qui ne sont attribués à aucun locataire, l'utilisateur peut les afficher si vous sélectionnez la valeur **Root tenant**.

Vous pouvez sélectionner la valeur **Root tenant** en plus de préciser les noms des locataires.

5. Dans la partie inférieure du bloc, cliquez sur le bouton **Generate**.

Le bloc **Token info** remplace le bloc **Generate token**.

6. Cliquez sur le bouton **Close** dans la partie inférieure du bloc **Token info**.

Le jeton d'actualisation que vous avez créé s'affiche dans la liste **All tokens**. Maintenant, vous pouvez utiliser ce jeton d'actualisation pour [créer un jeton d'accès](#).

Modification d'une connexion API dans Kaspersky Security Center

Vous pouvez modifier les connexions API existantes.

Pour modifier une connexion API :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **API**.

La liste des **API** s'affiche.

2. Cliquez sur la connexion API que vous souhaitez modifier.

Un bloc contenant les informations de connexion apparaît.

3. Modifiez les paramètres de connexion.

4. Cliquez sur **Enregistrer**.

Les nouveaux paramètres de la connexion API sélectionnée sont enregistrés.

Modification d'une connexion API dans la Console MDR en ligne

Vous pouvez modifier les connexions API existantes.

Pour modifier une connexion API :

1. Dans la Console MDR en ligne, cliquez sur l'onglet **API**.

La liste **All tokens** s'affiche.

2. Cliquez sur le jeton de connexion API que vous souhaitez modifier.

Un bloc contenant les informations de connexion apparaît.

3. Modifiez les paramètres de connexion.

4. Cliquez sur **Save**.

Les nouveaux paramètres de la connexion API sélectionnée sont enregistrés.

Création d'un jeton d'accès à Kaspersky Security Center

Un *jeton d'accès* est une séquence unique de caractères (lettres, chiffres et caractères spéciaux) qui vous permet d'utiliser les méthodes de l'API REST.

Pour créer un jeton d'accès, procédez comme suit :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **API**.

La liste des **API** s'affiche.

2. Cliquez sur une connexion avec un état **En attente d'activation**.

Un bloc contenant les informations de connexion apparaît.

3. Dans le champ **Jeton JWT**, cliquez sur le bouton **Actualiser**.

Un jeton d'actualisation s'affiche.

4. Sélectionnez et enregistrez la valeur du champ **Identifiant du client**.

5. Sélectionnez et enregistrez la séquence de caractères du jeton dans le presse-papiers.

6. Envoyez une requête POST au terminal `/session/confirm`.

Remplacez `{client_id}` et `{refresh_token}` par les valeurs sélectionnées et enregistrées dans les étapes précédentes.

Exemple (Python) :

```
#####
# Partie générale
#####

import time
import datetime
import requests
import jwt

# Le certificat est requis pour l'authentification d'une ressource externe
# Vous pouvez télécharger le certificat à l'adresse https://mdr.kaspersky.com,
# enregistrez-le sur votre disque et ajoutez son chemin dans la variable :
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# L'identifiant de votre client et vos jetons.
# Pour en savoir plus sur l'obtention de votre identifiant et des jetons, consultez l'aide https://support.kaspersky.com/MDR/fr-FR/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Collez la valeur)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Collez la valeur)
ACCESS_TOKEN = "AcCeSsToKeN" # (Collez la valeur)

#####
# Obtenir un jeton d'accès et un jeton d'actualisation pour la prochaine mise à jour du jeton d'accès
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN date et heure d'expiration: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN existe")
    else:
        print(
            "Vous devez mettre à jour REFRESH_TOKEN; Veuillez le récupérer depuis la Console MDR en ligne (https://support.kaspersky.com/MDR/fr-FR/258285.htm)"
        )
        exit()
else:
    print(
        "Vous devez renseigner la valeur REFRESH_TOKEN ; Veuillez la récupérer depuis la Console MDR en ligne (https://support.kaspersky.com/MDR/fr-FR/258285.htm)"
    )
    exit()

# Vérifier la présence et la validité du jeton d'accès
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN date et heure d'expiration: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN existe")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Si nécessaire, mettre à jour le jeton d'accès et actualiser le jeton pour la prochaine mise à jour du jeton d'accès
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    # Il est nécessaire d'enregistrer le jeton d'actualisation afin d'obtenir le prochain jeton d'accès après l'expiration du jeton d'accès actuel
    refresh_token = result_json["refresh_token"]
    print(
        f"Votre nouveau REFRESH_TOKEN pour votre prochaine demande ACCESS_TOKEN (veuillez remplacer la valeur de REFRESH_TOKEN par celle-ci): "
        f"{refresh_token}"
    )

    # Un nouveau jeton d'accès est requis pour récupérer les données
    access_token = result_json["access_token"]
    print(f"Votre nouveau ACCESS_TOKEN (veuillez remplacer la valeur de ACCESS_TOKEN par celle-ci) : \"{access_token}\"")

# Le jeton d'accès est ajouté à l'en-tête de la requête
headers = {"Authorization": f"Bearer {access_token}"}
```

Exemple (shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

L'API REST envoie une réponse comprenant le jeton d'accès et un nouveau jeton d'actualisation.

```
{
  "access_token": "SamPLET346yoKEsAmPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOKEsAmPLEt2590KEsS123aMPLe926tOkEnSaMPLe"
}
```

Maintenant, vous pouvez envoyer des requêtes à l'API REST en utilisant le jeton d'accès. Chaque requête à l'API REST nécessite un jeton d'accès ; une demande sans jeton d'accès ne renverra qu'une erreur d'autorisation.

Vous pouvez également [créer un jeton d'accès dans la Console MDR en ligne](#).

Création d'un jeton d'accès dans la Console MDR en ligne

Pour créer un jeton d'accès, procédez comme suit :

1. Dans la fenêtre de la Console MDR en ligne, accédez à l'option du menu **Settings**.

2. Cliquez sur l'onglet **API**.

La liste **All tokens** s'affiche. Chaque ligne représente un jeton. Vous pouvez cliquer n'importe où sur la ligne pour afficher les informations relatives au jeton.

3. Cliquez sur un jeton avec un état **Pending activation**.

Un bloc **Token info** s'affiche.

4. Dans le champ **JWT token**, cliquez sur le bouton **Actualiser**.

Un jeton d'actualisation s'affiche.

5. Sélectionnez et enregistrez la valeur du champ **Client ID**.

6. Sélectionnez et enregistrez la séquence de caractères du jeton dans le presse-papiers.

7. Envoyez une requête POST au terminal `/session/confirm` (voir les exemples ci-dessous).

Remplacez `{client_id}` et `{refresh_token}` par les valeurs sélectionnées et enregistrées dans les étapes précédentes.

Exemple (Python) :

```
#####
# Partie générale
#####

import time
import datetime
import requests
import jwt

# Le certificat est requis pour l'authentification d'une ressource externe
# Vous pouvez télécharger le certificat à l'adresse https://mdr.kaspersky.com,
# enregistrez-le sur votre disque et ajoutez son chemin dans la variable :
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# L'identifiant de votre client et vos jetons.
# Pour en savoir plus sur l'obtention de votre identifiant et des jetons, consultez l'aide https://support.kaspersky.com/MDR/fr-FR/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Collez la valeur)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Collez la valeur)
ACCESS_TOKEN = "AcCeSsToKeN" # (Collez la valeur)

#####
# Obtenir un jeton d'accès et un jeton d'actualisation pour la prochaine mise à jour du jeton d'accès
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN date et heure d'expiration: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN existe")
    else:
        print(
            "Vous devez mettre à jour REFRESH_TOKEN; Veuillez le récupérer depuis la Console MDR en ligne (https://support.kaspersky.com/MDR/fr-FR/258285.htm)"
        )
        exit()
else:
    print(
        "Vous devez renseigner la valeur REFRESH_TOKEN ; Veuillez la récupérer depuis la Console MDR en ligne (https://support.kaspersky.com/MDR/fr-FR/258285.htm)"
    )
    exit()

# Vérifier la présence et la validité du jeton d'accès
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN date et heure d'expiration: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN existe")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Si nécessaire, mettre à jour le jeton d'accès et actualiser le jeton pour la prochaine mise à jour du jeton d'accès
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    # Il est nécessaire d'enregistrer le jeton d'actualisation afin d'obtenir le prochain jeton d'accès après l'expiration du jeton d'accès actuel
    refresh_token = result_json["refresh_token"]
    print(
        f"Votre nouveau REFRESH_TOKEN pour votre prochaine demande ACCESS_TOKEN (veuillez remplacer la valeur de REFRESH_TOKEN par celle-ci): "
        f"{refresh_token}"
    )

    # Un nouveau jeton d'accès est requis pour récupérer les données
    access_token = result_json["access_token"]
    print(f"Votre nouveau ACCESS_TOKEN (veuillez remplacer la valeur de ACCESS_TOKEN par celle-ci) : \"{access_token}\"")

# Le jeton d'accès est ajouté à l'en-tête de la requête
headers = {"Authorization": f"Bearer {access_token}"}
```

Exemple (shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

L'API REST envoie une réponse comprenant le jeton d'accès et un nouveau jeton d'actualisation.

```
{
  "access_token": "SamPLET346yoKEsAmPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOKEsAmPLEt2590KEsS123aMPLe926t0KEsAmPLE"
}
```

Maintenant, vous pouvez envoyer des requêtes à l'API REST en utilisant le jeton d'accès. Chaque requête à l'API REST nécessite un jeton d'accès ; une demande sans jeton d'accès ne renverra qu'une erreur d'autorisation.

Utilisation de l'API REST

Utilisez MDR via l'API REST pour obtenir, créer et mettre à jour des ressources, des incidents, des réponses et des utilisateurs.

[OUVRIR LA RÉFÉRENCE DE L'API REST](#)

Les méthodes de l'API REST nécessitent la valeur `client_id`. Vous pouvez récupérer votre valeur `client_id` dans le bloc **Token info** de n'importe quel jeton d'actualisation dans la Console MDR en ligne.

Voici des exemples de script pour Python et Shell qui illustrent les fonctionnalités de base de l'API REST :

- Définir le chemin du certificat, l'URL de l'API REST, l'ID client et les jetons
- Obtenir le jeton d'accès et le jeton d'actualisation pour la prochaine mise à jour du jeton d'accès
- Obtenir le numéro de la ressource
- Obtenir la liste des ressources ou les détails de la ressource
- Obtenir le nombre d'incidents, la liste des incidents ou les détails de l'incident
- Obtenir la liste des réponses correspondant à l'incident
- Confirmer, refuser la réponse ou mettre à jour la liste des réponses
- Obtenir la liste des commentaires pour l'incident spécifié ou créer un nouveau commentaire pour l'incident spécifié

Exemple (Python) :

```
#####
# Partie générale
#####

import time
import datetime
import requests
import jwt

# Le certificat est requis pour l'authentification d'une ressource externe
# Vous pouvez télécharger le certificat à l'adresse https://mdr.kaspersky.com,
# enregistrez-le sur votre disque et ajoutez son chemin dans la variable :
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# URL de l'API REST MDR :
API_URL = "https://mdr.kaspersky.com/api/v1"

# L'identifiant de votre client et vos jetons.
# Pour en savoir plus sur l'obtention de votre identifiant et des jetons, consultez l'aide https://support.kaspersky.com/MDR/fr-FR/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Collez la valeur)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Collez la valeur)
ACCESS_TOKEN = "AcCeSsToKeN" # (Collez la valeur)

#####
# Obtenir un jeton d'accès et un jeton d'actualisation pour la prochaine mise à jour du jeton d'accès
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN date et heure d'expiration : {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN existe")
    else:
        print(
            "Vous devez mettre à jour REFRESH_TOKEN; Veuillez le récupérer depuis la Console MDR (https://support.kaspersky.com/MDR/fr-FR/258285.htm)"
        )
        exit()
else:
    print(
        "Vous devez renseigner la valeur REFRESH_TOKEN ; Veuillez la récupérer depuis la Console MDR (https://support.kaspersky.com/MDR/fr-FR/258285.htm)"
    )
    exit()

# Vérifier la présence et la validité du jeton d'accès
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN date et heure d'expiration : {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN existe")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Si nécessaire, mettre à jour le jeton d'accès et actualiser le jeton pour la prochaine mise à jour du jeton d'accès
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    # Il est nécessaire d'enregistrer le jeton d'actualisation afin d'obtenir le prochain jeton d'accès après l'expiration du jeton d'accès actuel
    refresh_token = result_json["refresh_token"]
    print(
        f"Votre nouveau REFRESH_TOKEN pour votre prochaine demande ACCESS_TOKEN (veuillez remplacer la valeur de REFRESH_TOKEN par celle-ci) : "
        f"{refresh_token}"
    )

    # Un nouveau jeton d'accès est requis pour récupérer les données
    access_token = result_json["access_token"]
    print(f"Votre nouveau ACCESS_TOKEN (veuillez remplacer la valeur de ACCESS_TOKEN par celle-ci) : \"{access_token}\"")

# Le jeton d'accès est ajouté à l'en-tête de la requête
headers = {"Authorization": f"Bearer {access_token}"}
```

```
#####
# Obtenir le nombre de ressources
#####

# La date et l'heure sont exprimées en millisecondes depuis 1970-01-01T00:00:00Z
request_body = {
    "max_last_seen": int(time.time())
    * 1000, # Limiter la durée maximale de la dernière apparition de la ressource à l'heure actuelle
    "min_last_seen": 163931132000, # Limiter la durée de la dernière apparition de la ressource avec la constante - Dimanche 12 décembre 2021 12:12:12
    (GMT)
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtenir la liste des ressources
#####

request_body = {
    # Paramètres de recherche :
    "version": 2, # Spécifiez 2 comme version de la solution
    "max_last_seen": int(time.time())
    * 1000, # Limiter la durée maximale de la dernière apparition de la ressource à l'heure actuelle
```

```

"min_last_seen": 1639311132000, # Limiter la durée de la dernière apparition de la ressource avec la constante - Dimanche 12 décembre 2021 12:12:12
(GMT)
"domain": "",
"host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"], # (Collez la valeur) Liste des noms d'hôtes
"is_isolated": False,
"network_interface": "10.70.104.1",
"os_version": "Windows", # La ressource doit contenir la ligne indiquée dans le nom du système d'exploitation
"product": "",
"search_phrase": "mdr", # Phrase à rechercher en fonction du contenu des champs : "host_name", "domain", "installed_product_info",
"network_interfaces", "os_version"
"statuses": ["OK", "ABSENT"], # Rechercher des ressources dont l'état actuel est indiqué ici
# Options d'affichage des résultats de la recherche :
"sort": "first_seen:asc", # Trier les résultats en fonction de l'heure de la première occurrence ; dans le cas où les résultats sont affichés page
par page, il est nécessaire d'indiquer un champ de tri qui ne changera pas d'une requête à l'autre, par exemple, "first_seen" (ne pas indiquer de champs
dont les valeurs changent constamment, par exemple le champ "last_seen" ; les résultats obtenus pourraient être erronés)
"page_size": 100, # Nombre de ressources par page - 100
"page": 1, # Affiche la première page des résultats de recherche
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtenir les détails de la ressource
#####

request_body = {
    "version": 2, # Spécifiez 2 comme version de la solution
    "asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", # (Collez la valeur) ID de la ressource
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
).json()
print(result)

#####
# Obtenir le nombre d'incidents
#####

request_body = {
    "max_update_time": int(time.time())
    * 1000, # Limiter la durée de la dernière mise à jour de l'incident à l'heure actuelle
    "min_update_time": 1639311132000, # Limiter l'heure minimale de la dernière mise à jour de l'incident avec la constante - dimanche 12 décembre 2021
12:12:12 (GMT)
    "affected_hosts": [
        "MA-MDR-KES-S:0xFA6A68CC9A94145456E841048A3BE929"
    ], # (Collez la valeur) Liste des hôtes au format "host_name:asset_id"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtenir la liste des incidents
#####

request_body = {
    # Paramètres de recherche :
    "max_creation_time": int(time.time())
    * 1000, # Limiter la durée de création de l'incident à l'heure actuelle
    "min_creation_time": 1639311132000, # Limiter la durée minimale pour la création d'un incident avec la constante -Dimanche 12 décembre 2021
12:12:12 (GMT)
    "asset_ids": [
        "0xFA6A68CC9A9415963DE841048A3BE929"
    ], # (Collez la valeur) Liste des ressources pour lesquelles nous obtenons des incidents
    "priorities": ["HIGH"],
    "resolutions": ["True positive"],
    "response_statuses": ["Confirmed"],
    "response_types": ["hash"],
    "statuses": ["Closed"],
    # Paramètres d'obtention des résultats
    "markdown_to_html": True, # Résultats au format HTML ; si la valeur est "False", les résultats sont au format Markdown
    "sort": "creation_time:asc", # Trier les résultats en fonction de la date et de l'heure de la création de l'incident ; dans le cas où les résultats
sont affichés page par page, il est nécessaire d'indiquer un champ de tri qui ne changera pas d'une requête à l'autre, par exemple, « creation_time »
(ne pas indiquer de champs dont les valeurs changent constamment, par exemple le champ « update_time » ; les résultats obtenus pourraient être erronés)
    "page_size": 100, # Nombre d'incidents par page - 100
    "page": 1, # Affiche la première page des résultats de recherche
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtenir les détails de l'incident
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Collez la valeur) ID de l'incident
    "markdown_to_html": True, # Résultats au format HTML ; si la valeur est « False », les résultats sont au format Markdown
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtenir la liste des réponses à l'incident
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Collez la valeur) ID de l'incident
    "page_size": 10, # Nombre de réponses par page - 10
    "page": 1, # Affiche la première page des résultats de recherche
}

```

```

result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Confirmer la réponse
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Collez la valeur) ID de la réponse
    "comment": "comment_text", # Commentaire à ajouter à la réponse
    "status": "Confirmed", # Nouvel état de la réponse - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Refuser la réponse
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Collez la valeur) ID de la réponse
    "comment": "comment_text", # Commentaire à ajouter à la réponse
    "status": "Declined", # Nouvel état de la réponse - "Declined"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Mettre à jour la liste des réponses
#####

request_body = {
    "responses_ids": [
        "CEgYG4UBMUGN-LWULP7W",
        "2ES16IgB4cAOUyXBb5IB",
    ], # (Collez les valeurs) ID des réponses
    "comment": "comment_text", #Commentaire à ajouter aux réponses
    "status": "Confirmed", # Nouvel état des réponses - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

```

Exemple (shell) :

```
# Obtenir un jeton d'accès et un nouveau jeton d'actualisation
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
# Exemple de réponse ; Ensuite, vous devez utiliser la valeur « access_token » pour récupérer les données et la valeur « refresh_token » pour récupérer
le nouveau jeton d'accès et le jeton d'actualisation
{
  "access_token": "SamPLET346yoKEsSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPleT2590KEsS123aMPle926tOkEnSaMPle"
}

# Obtenir le nombre de ressources
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/count -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d
'{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000}'

# Obtenir la liste des ressources
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/list -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d
'{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000, "domain": "", "host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"], "is_isolated": false,
"network_interface": "10.70.104.1", "os_version": "Windows", "product": "", "search_phrase": "mdr", "statuses": ["OK", "ABSENT"], "sort":
"first_seen:asc", "page_size": 100, "page": 1, "version": 2}'

# Obtenir les détails de la ressource
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/details -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -
d '{"asset_id": "0xFA68CC9A9415963DE841048A3BE929", "version": 2}'

# Obtenir le nombre d'incidents
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/count -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}"
-d '{"max_update_time": 1704103200000, "min_update_time": 1704762000000, "affected_hosts": ["MA-MDR-KES-S:0xFA68CC9A9415963DE841048A3BE929"]}'

# Obtenir la liste des incidents
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/list -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -
d '{"max_creation_time": 1704103200000, "min_creation_time": 1704762000000, "asset_ids": ["0xFA68CC9A9415963DE841048A3BE929"], "priorities": ["HIGH"],
"resolutions": ["True positive"], "response_statuses": ["Confirmed"], "response_types": ["hash"], "statuses": ["Closed"], "markdown_to_html": true,
"sort": "creation_time:asc", "page_size": 100, "page": 1}'

# Obtenir les détails de l'incident
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/details -H "Content-Type: application/json" -H "Authorization: Bearer
{access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "markdown_to_html": true}'

# Obtenir la liste des réponses à l'incident
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/list -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -
d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "page_size": 10, "page": 1}'

# Mettre à jour la réponse
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/response/update -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}"
-d '{"response_id": "CEgYG4UBMUGN-LWULP7W", "comment": "comment_text", "status": "Confirmed"}'

# Mettre à jour la liste des réponses
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/update -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}"
-d '{"responses_ids": ["CEgYG4UBMUGN-LWULP7W", "2ES16IgB4cA0UyXBb5IB"], "comment": "comment_text", "status": "Confirmed"}'
```

Exemple de réponse de l'API REST avec le jeton d'accès et le nouveau jeton d'actualisation :

```
{
  "access_token": "SamPLET346yoKEsSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPleT2590KEsS123aMPle926tOkEnSaMPle"
}
```

Exemple de réponse de l'API REST avec la structure et les valeurs des commentaires :

```
[{
  "comment_id": "bfu6TiNghqp",
  "author_name": "Jean Paillet",
  "text": "<p>Le premier commentaire</p>",
  "creation_time": 1601295428640
}, {
  "comment_id": "bfu6TiNghqt",
  "author_name": "Jeanne Paillet",
  "text": "<p>Le deuxième commentaire</p>",
  "creation_time": 1601295433441
}]
```

Exemple de réponse de l'API REST lorsque l'API REST crée un nouveau commentaire et envoie une réponse avec les détails du commentaire :

```
{
  "comment_id": "AXTej0Qi4bfu6TiNgmvT",
```

```
"author_name": "Nom du jeton",  
"text": "Ceci est un nouveau commentaire créé via l'API REST",  
"creation_time": 1601461748122  
}
```

Révocation du jeton d'actualisation dans Kaspersky Security Center

Vous pouvez révoquer les jetons d'actualisation des connexions API qui ont actuellement le statut *Actif* ou *Inactif*.

Pour créer un jeton d'actualisation :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **API**.
La liste des **API** s'affiche.
2. Cliquez sur la connexion API à partir de laquelle vous souhaitez révoquer un jeton d'actualisation.
Un bloc contenant les informations de connexion apparaît.
3. Cliquez sur le bouton **Révoquer**.
Le jeton d'actualisation est révoqué.

Suppression d'une connexion API dans Kaspersky Security Center

Vous pouvez supprimer les connexions API existantes.

Pour supprimer une connexion API :

1. Dans la section **MDR** de Kaspersky Security Center, cliquez sur l'onglet **API**.
La liste des **API** s'affiche.
2. Sélectionnez le bouton radio situé à côté de la connexion API que vous souhaitez supprimer, puis cliquez sur **Supprimer la connexion**.
La connexion API sélectionnée est supprimée.

Suppression d'une connexion API dans la Console MDR en ligne

Vous pouvez modifier les connexions API existantes.

Pour modifier une connexion API :

1. Dans la Console MDR en ligne, cliquer sur l'onglet **API**.

La liste **All tokens** s'affiche.

2. Pointez sur la connexion API que vous souhaitez supprimer, puis cliquez sur l'icône de la corbeille () sur le côté droit de la ligne.

La connexion API sélectionnée est supprimée.

Désactivation de Kaspersky Managed Detection and Response

Si vous souhaitez cesser d'utiliser Kaspersky Managed Detection and Response, vous pouvez soit mettre fin à son utilisation de manière permanente, soit la suspendre temporairement sur certaines ressources.

Arrêt de l'utilisation de Kaspersky Managed Detection and Response

Vous pouvez arrêter l'utilisation de Kaspersky Managed Detection and Response manuellement si vous le souhaitez.

Lorsque vous mettez fin à l'utilisation de Kaspersky Managed Detection and Response, la solution cesse d'envoyer des données télémétriques à partir de vos ressources. Pour supprimer les données concernant votre organisation de l'infrastructure de Kaspersky Managed Detection and Response, veuillez contacter [le Support Technique](#).

Pour mettre fin à l'utilisation de Kaspersky Managed Detection and Response :

1. Dans Kaspersky Security Center Web Console ou Kaspersky Next Expert View, accédez à la section **Ressources (Appareils)** → **Stratégies et profils** si vous utilisez les [applications EPP](#) qui prennent en charge les stratégies.

Si vous utilisez une application EPP qui ne prend pas en charge les politiques, accédez à la section **Ressources (Appareils)** → **Tâches**.

La liste des stratégies (ou la liste des tâches) s'ouvre.

2. Cliquez sur une politique ou une tâche que vous avez créée lors du déploiement de Kaspersky Managed Detection and Response pour configurer l'intégration entre une application EPP et Kaspersky Managed Detection and Response.

La fenêtre des paramètres de stratégie (ou la fenêtre des paramètres de tâche) s'ouvre.

3. Dans l'onglet **Paramètres de l'application** dans le volet de gauche, sélectionnez **Detection and Response**, puis dans le volet de droite, sélectionnez **Managed Detection and Response**.

Le volet des paramètres de **Managed Detection and Response**.

4. Désactivez l'option **Détection et réponse gérées activées**.

Le nom de l'option devient **Managed Detection and Response désactivée**.

5. Enregistrez les modifications apportées à la stratégie ou à la tâche.

6. [Révoquez de votre consentement avec les conditions d'utilisation de la solution MDR](#).

7. Si vous utilisez Kaspersky Security Center Web Console pour travailler avec Kaspersky MDR, il est en outre recommandé de [supprimer le fichier de configuration KPSN du Serveur d'administration de Kaspersky Security Center](#) [☞].

L'utilisation de Kaspersky Managed Detection and Response s'arrête.

Suspension de l'utilisation de Kaspersky Managed Detection and Response

Pour se conformer aux [conditions d'utilisation de la solution MDR](#), il est nécessaire de suspendre l'utilisation de la solution sur les ressources si ces dernières se trouvent temporairement sur le territoire des États-Unis (par exemple, à l'occasion d'un déplacement professionnel).

Pour suspendre temporairement l'utilisation de la solution MDR sur certaines ressources, procédez comme suit :

1. Dans Kaspersky Security Center, créez un nouveau [groupe d'administration](#) [☞] pour gérer les ressources sur lesquelles vous souhaitez suspendre l'utilisation de la solution MDR. Vous pourrez modifier la liste des ressources de ce groupe ultérieurement.
2. Pour ce groupe d'administration, [créez les nouvelles stratégies](#) [☞] des applications EPP utilisées pour transmettre la télémétrie MDR depuis des ressources, puis désactivez l'utilisation de la solution MDR et de Kaspersky Security Network dans les paramètres de la stratégie.

Pour en savoir plus sur la configuration des stratégies, consultez les articles d'aide d'une application EPP en particulier. Par exemple, l'aide de Kaspersky Endpoint Security for Windows contient des instructions sur [l'administration des stratégies](#) [☞] et de configuration de [l'intégration à la solution MDR](#) [☞].

3. [Déplacez les ressources](#) [☞] pour lesquelles vous souhaitez suspendre l'utilisation de la solution MDR au groupe d'administration créé.

La nouvelle stratégie, qui désactive l'utilisation de la solution MDR et de Kaspersky Security Network, sera appliquée aux ressources après la synchronisation. Vous pouvez aussi [forcer la synchronisation](#) [☞] manuellement.

Pour reprendre l'utilisation de Kaspersky Managed Detection and Response après la suspension, procédez comme suit :

1. Excluez la ressource du groupe d'administration utilisé pour la suspension.
2. Appliquez une stratégie standard selon laquelle l'utilisation de la solution MDR est activée et configurée pour cette ressource.

Les ressources ne seront pas surveillées par la solution MDR tant qu'une stratégie selon laquelle l'utilisation de la solution MDR est activée et configurée leur est appliquée.

Révocation de votre consentement avec les conditions d'utilisation de la solution MDR

Si vous décidez d'arrêter d'utiliser Kaspersky Managed Detection and Response, révoquez votre consentement avec les conditions d'utilisation de la solution MDR, puis [désactivez l'utilisation de Kaspersky Managed Detection and Response sur les ressources](#).

Cette fonctionnalité n'est disponible que si vous avez défini le droit d'accès **Intégration d'applications** dans [Kaspersky Security Center Web Console](#) ou [Kaspersky Next Expert View](#).

Pour révoquer votre consentement avec les conditions d'utilisation de la solution MDR, procédez comme suit :

1. Pour ce faire, dans la section MDR de la fenêtre de Kaspersky Security Center, cliquez sur l'onglet **Utilisation de MDR**.
2. Développez le groupe **Conditions d'utilisation de la solution MDR** en cliquant sur son nom.
3. Cliquez sur le lien **Révoquer la confirmation de l'acceptation des conditions d'utilisation de la solution MDR**.
4. Confirmez que vous souhaitez révoquer votre consentement avec les conditions d'utilisation de la solution MDR.

Votre consentement aux conditions d'utilisation de la solution MDR est révoqué.

Si vous souhaitez supprimer les informations sur votre organisation de l'infrastructure MDR, veuillez contacter le [Support Technique](#).

Problèmes connus

Kaspersky Managed Detection and Response présente une série de restrictions qui n'ont pas une incidence critique sur le fonctionnement de l'application :

- Si vous clonez une ressource virtuelle ou physique avec Kaspersky Endpoint Security for Linux déjà connecté à la solution MDR, les données de télémétrie des ressources clonées ne sont pas transmises correctement. Pour ces ressources clonées, supprimez Kaspersky Endpoint Security for Linux, supprimez le fichier `install_id` se trouvant dans le dossier `/var/opt/kaspersky/epagent/`, puis réinstallez Kaspersky Endpoint Security for Linux.
- En ce qui concerne les ressources de Kaspersky Endpoint Security for Windows disponibles dans la configuration de Endpoint Detection and Response Agent (EDR Agent), les états *Avertissement* et *Critique* des composants de protection et de contrôle ne sont pas affichés.
- Vous ne pouvez pas utiliser les fonctionnalités de [Kaspersky Endpoint Detection and Response Optimum](#) pour les ressources associées à Kaspersky Endpoint Security for Windows dans la configuration de EDR Agent.
- Les **applications Kaspersky compatibles avec la section MDR** de la fiche des ressources dans la Console MDR en ligne peuvent contenir des applications Endpoint Protection Platform (EPP) obsolètes, qui ne sont plus utilisées pour fonctionner avec Kaspersky Managed Detection and Response. Cela se produit lorsqu'une application EPP obsolète a été remplacée par une nouvelle sur la ressource. Pour ces applications obsolètes, le champ **Vu pour la dernière fois** contient l'ancienne date, tandis que pour la nouvelle application EPP, le champ **Vu pour la dernière fois** contient la date la plus récente.
- La solution MDR qui utilise la configuration KPSN ne prend pas en charge une hiérarchie des Serveurs d'administration de Kaspersky Security Center si seul le serveur principal de la hiérarchie a accès à Internet.
- La solution MDR ne prend pas en charge le téléchargement automatique de fichiers de plus de 64 Mo lors de l'utilisation de la [réponse Get artefacts](#) disponible via Kaspersky Endpoint Detection and Response Expert, intégré à la plateforme Open Single Management Platform.
- Le plug-in MDR pour Kaspersky Security Center et le plug-in MDR pour Open Single Management Platform ne prennent pas en charge l'affichage des informations relatives à Kaspersky Embedded Systems Security pour Linux version 4.0 ou ultérieure dans la liste des ressources inactives.

Contacter le Support Technique

Cette section décrit comment bénéficier du support technique et les conditions de cette obtention.

Modes d'obtention du support technique

Si vous ne trouvez pas de solution à votre problème dans la documentation de [Kaspersky Managed Detection and Response](#) ou dans l'une des sources d'informations sur [Kaspersky Managed Detection and Response](#), contactez le Service client de Kaspersky. Les experts du Support Technique répondront à l'ensemble de vos questions sur l'installation et l'utilisation de Kaspersky Managed Detection and Response.

Kaspersky prend en charge Kaspersky Managed Detection and Response pendant son cycle de vie (voir la [page du cycle de vie de l'assistance relative aux applications](#)). Avant de contacter le Support Technique, il est recommandé de lire les [règles d'octroi du Support Technique](#).

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- [En visitant le site Internet du Support Technique](#)
- En envoyant une demande au Support Technique à partir du [portail Kaspersky CompanyAccount](#)

Assistance technique via le Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) est un portail dédié aux entreprises utilisant les applications Kaspersky. Le portail Kaspersky CompanyAccount vise à permettre l'interaction entre les utilisateurs et les spécialistes de Kaspersky via des requêtes en ligne. Vous pouvez utiliser Kaspersky CompanyAccount pour suivre l'état des requêtes en ligne et en stocker également un historique.

Vous pouvez enregistrer tous les employés de votre entreprise dans un seul compte utilisateur Kaspersky CompanyAccount. Ce compte utilisateur unique vous permet de centraliser l'administration des requêtes électroniques envoyées à Kaspersky et provenant des employés enregistrés. Il vous permet également d'administrer les privilèges de ces employés Kaspersky CompanyAccount.

Le portail Kaspersky CompanyAccount est disponible dans les langues suivantes :

- Anglais
- Espagnol
- Italien
- Allemand
- Polonais
- Portugais

- Russe
- Français
- Japonais

Pour en savoir plus sur le Kaspersky CompanyAccount, veuillez consulter le [site Internet du Service de Support Technique](#) .

Sources d'informations à propos de la solution

Sur la page [Kaspersky Managed Detection and Response](#), vous pouvez afficher des informations générales sur la solution, ses fonctions et ses caractéristiques.

Glossaire

Application EPP

Une application incluse dans un système de protection pour les terminaux (Plateforme de protection des terminaux ou EPP). Les applications EPP sont installées sur des terminaux au sein de l'infrastructure informatique d'une organisation (par exemple, des appareils mobiles, des ordinateurs ou des ordinateurs portables). Un exemple d'application EPP est Kaspersky Endpoint Security for Windows dans le cadre de la solution EPP Kaspersky Endpoint Security for Business.

Incident

Une activité évaluée comme critique par la technologie de détection et qui nécessite une réaction immédiate de Kaspersky Managed Detection and Response.

IOC

Un indicateur de compromission (ou IOC) montre la preuve sur un appareil qu'il existe une faille de sécurité.

Locataire

Un locataire est une organisation à laquelle vous fournissez Kaspersky Managed Detection and Response.

Plateforme de protection des terminaux (EPP)

Un système intégré de protection complexe pour les terminaux (par exemple, les appareils mobiles, les ordinateurs ou les ordinateurs portables) qui inclut diverses technologies de sécurité. Kaspersky Endpoint Security for Business est un exemple de plateforme de protection des terminaux.

Réponse

La réponse aux incidents est une méthodologie structurée permettant de gérer les incidents de sécurité, les violations et les cybermenaces.

Ressource

Un appareil avec une application Kaspersky EPP installée (par exemple, Kaspersky Endpoint Security for Windows).

Tactique MITRE

L'objectif qu'un attaquant voulait atteindre lors d'une cyberattaque sur l'infrastructure du Client.

Technique MITRE

Méthode utilisée par l'attaquant pour effectuer des actions malveillantes lors d'une cyberattaque sur l'infrastructure cliente. Chaque tactique MITRE contient un ensemble de techniques MITRE.

Télémétrie

Données envoyées depuis les ressources vers Kaspersky Managed Detection and Response.

Informations sur le code tiers

Un code tiers a été utilisé dans le développement de la solution.

Pour en savoir plus à propos du code tiers dans la Console MDR en ligne, contactez le support Kaspersky Managed Detection and Response.

Les informations relatives au code tiers utilisé dans le plug-in MDR figurent dans le fichier [legal_notices.txt](#).

Avis de marques commerciales

Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs.

Apple, Mac, macOS et Safari sont des marques commerciales d'Apple Inc.

Amazon AWS et Amazon Web Services sont des marques commerciales d'Amazon.com, Inc. ou de ses sociétés affiliées.

Active Directory, Internet Explorer, Microsoft, Microsoft Edge, Outlook, PowerShell, Windows PowerShell, Windows et Windows Server sont des marques commerciales du groupe de sociétés Microsoft.

Firefox et Mozilla sont des marques commerciales Mozilla Foundation aux États-Unis et dans d'autres pays.

Google et Google Chrome sont des marques commerciales de Google LLC.

Linux est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

Python est une marque commerciale ou une marque déposée de la Python Software Foundation.

Configuration de la stratégie d'audit des événements Windows à utiliser avec Kaspersky Managed Detection and Response

Pour garantir un fonctionnement stable et optimiser l'efficacité de Kaspersky Managed Detection and Response, nous vous recommandons de configurer les paramètres d'audit suivants :

- Pour configurer la stratégie d'audit des événements Windows, procédez comme suit :

Pour maximiser l'efficacité de Kaspersky Managed Detection and Response, vous devez configurer la stratégie d'audit des événements Windows sur vos ressources.

Pour configurer la stratégie d'audit des événements Windows, procédez comme suit :

1. Sur les ressources fonctionnant sous Windows, appuyez sur **Win+R** pour ouvrir la fenêtre **Exécuter**.
2. Dans le champ **Ouvrir**, saisissez `gpedit.msc`, puis appuyez sur **Entrée** ou cliquez sur **OK**. La fenêtre **Éditeur de stratégie de groupe local** s'affiche.
3. Dans l'arborescence de la console, cliquez sur **Configuration de l'ordinateur** → **Paramètres Windows** → **Paramètres de sécurité** → **Configuration avancée de la stratégie d'audit** → **Stratégies d'audit système** – **Objet de stratégie de groupe local**.
4. Cliquez sur le nœud **Connexion du compte**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Auditer la validation des identifiants	Succès et échec
Auditer le service d'authentification Kerberos	Succès et échec
Auditer les opérations des tickets d'assistance Kerberos	Succès et échec

5. Cliquez sur le nœud **Gestion du compte**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Auditer la gestion des comptes utilisateurs	Succès et échec
Gestion des groupes de sécurité d'audit	Succès
Gestion des comptes utilisateurs d'audit	Succès et échec

6. Cliquez sur le nœud **Accès au service d'annuaire**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Auditer l'accès au service d'annuaire	Succès et échec
Auditer les modifications du service d'annuaire	Succès et échec

7. Cliquez sur le nœud **Connexion/Déconnexion**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Verrouillage du compte d'audit	Échec
Connexion d'audit	Succès et échec
Auditer les connexions spéciales	Succès et échec

8. Cliquez sur le nœud **Accès aux objets**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Services d'audit et de certification	Succès et échec
Partage de fichiers d'audit	Succès
Connexion à la plateforme de filtrage d'audit	Succès
Autres événements d'accès aux objets d'audit	Succès

9. Cliquez sur le nœud **Changement de stratégie**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Changement de la stratégie d'audit	Succès
Changement de la stratégie d'audit au niveau de la règle MPSSVC	Succès

10. Cliquez sur le nœud **Utilisation des privilèges**. Définissez la valeur suivante dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Utilisation des privilèges sensibles d'audit	Succès

11. Cliquez sur le nœud **Système**. Définissez les valeurs suivantes dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Changement de l'état de sécurité d'audit	Succès
Extension du système de sécurité d'audit	Succès

12. Dans l'arborescence de la console, cliquez sur le bouton **Configuration de l'ordinateur → Modèles d'administration → Composants Windows → Windows PowerShell**. Définissez la valeur suivante dans la partie droite de la fenêtre :

Sous-catégorie	Événements d'audit
Activer la journalisation des blocs de scripts PowerShell	Activée

13. Fermez la fenêtre **Éditeur de stratégie de groupe local**.

Toutes les modifications sont enregistrées automatiquement.

La stratégie d'audit des événements Windows est désormais configurée pour utiliser Kaspersky Managed Detection and Response.

• Configuration de l'audit des objets Active Directory

Pour maximiser l'efficacité de Kaspersky Managed Detection and Response, vous devez configurer l'audit sur vos contrôleurs de domaine Windows.

Pour configurer l'audit des objets Active Directory :

1. Sur votre contrôleur de domaine Windows, appuyez sur **Win+R** pour ouvrir la fenêtre **Exécuter**.
2. Dans le champ **Ouvrir**, saisissez `dsa.msc`, puis appuyez sur **Entrée** ou cliquez sur **OK**. La fenêtre **Utilisateurs et ordinateurs Active Directory** s'affiche.
3. Dans l'arborescence de la console, faites un clic droit sur <votre nom de domaine>, puis sélectionnez **Rechercher**. La fenêtre **Recherche d'utilisateurs, de contacts et de groupes** s'ouvre.
4. Saisissez **Administrateur** dans le champ **Nom**, puis cliquez sur **Rechercher**.
5. Dans la zone **Résultats de la recherche**, faites un clic droit sur l'objet **Administrateur**, puis sélectionnez **Propriétés** → **Sécurité** → **Avancé** – onglet **Audit**.
6. Cliquez sur **Ajouter** pour ouvrir la fenêtre **Audit de l'entrée pour l'administrateur**. Cliquez sur **Sélectionnez un principal**, saisissez `Tout le monde`, cliquez sur **Vérifier les noms**, puis sur **OK**.
7. Dans la fenêtre **Audit de l'entrée pour l'administrateur**, cochez les cases **Afficher le contenu**, **Autorisations de lecture**, **Autorisations de modification**, **Modifier le propriétaire**, **Propriétés en lecture** et en **Propriétés en écriture**.
8. Cliquez sur **OK** → **Appliquer** → **OK**.

L'audit pour l'**Administrateur** de l'objet Active Directory est désormais configuré pour être utilisé avec Kaspersky Managed Detection and Response.

9. Exécutez les mêmes étapes pour les objets Active Directory par défaut suivants, ainsi que pour les utilisateurs et groupes du domaine sensible, qui existent et sont activés dans votre système :

- **Administrateurs**
- **Groupe de réplication du mot de passe RODC autorisé**
- **Éditeurs de certificats**
- **Contrôleurs de domaine clonables**
- **Groupe de réplication de mot de passe RODC refusé**
- **DnsAdmins**
- **DnsUpdateProxy**
- **Administrateurs de domaine**
- **Ordinateurs de domaine**
- **Contrôleurs de domaine**
- **Administrateurs de l'entreprise**
- **Administrateurs clés de l'entreprise**
- **Contrôleurs de domaine en lecture seule de l'entreprise**

- Propriétaires créateurs de stratégie de groupe
- Administrateurs clés
- krbtgt
- Utilisateurs protégés
- Serveurs RAS et IAS
- Contrôleurs de domaine en lecture seule
- Administrateurs de schémas
- Configuration de l'audit pour les services de certificats Active Directory, les modèles de certificat et les objets de certificat

Pour optimiser l'efficacité de Kaspersky Managed Detection and Response, vous devez configurer l'audit pour le service **Services de certificats Active Directory**, les modèles de certificat et les objets sur les hôtes sur lesquels les services de certificats Active Directory (AD CS) sont activés.

*Pour configurer l'audit pour le service **Services de certificats Active Directory**, procédez comme suit :*

1. Appuyez sur **Win+R** pour ouvrir la fenêtre **Exécuter**.
2. Dans le champ **Ouvrir**, saisissez `cmd`, puis appuyez sur **Entrée** ou cliquez sur **OK**. La fenêtre **Invite de commandes** s'affiche.
3. Pour configurer les paramètres d'audit pour l'Autorité de certification, saisissez les commandes ci-dessous, puis appuyez sur la touche Entrée :
`certutil -setreg CA\AuditFilter 127`
`certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD`
4. Pour redémarrer le service **Services de certificats**, saisissez la commande ci-dessous et appuyez sur la touche Entrée :
`net stop certsvc && net start certsvc`

Pour configurer l'audit de sécurité pour les modèles de certificat, procédez comme suit :

1. Appuyez sur **Win+R** pour ouvrir la fenêtre **Exécuter**.
2. Dans le champ **Ouvrir**, saisissez `adsiedit.msc`, puis appuyez sur **Entrée** ou cliquez sur **OK**.
3. Cliquez avec le bouton droit de la souris sur **Modification ADSI** et sélectionnez **Se connecter à**.
4. Dans la section **Point de connexion**, sélectionnez la valeur **Configuration** dans le champ Sélectionnez un Contexte d'appellation connu.
5. Double-cliquez sur **Configuration/Schéma** dans le volet de gauche.
6. Sélectionnez le dossier **CN=Configuration,DC=...** → **CN=Services** → **CN=Service de clés publiques** → **CN=Modèles de certificats**.
7. Cliquez avec le bouton droit de la souris sur le dossier **CN=Modèles de certificats**, sélectionnez **Propriétés** puis ouvrez l'onglet **Sécurité**.

8. Cliquez sur le bouton **Avancé** et sélectionnez l'onglet **Audit**.
9. Cliquez sur la classe d'objet principal **Tout le monde**, cochez les cases **Propriétés en écriture**, **Supprimer**, **Modifier les permissions**, **Modifier le propriétaire**, **Toutes les écritures validées**, puis cliquez sur **OK**.

Pour configurer l'audit de sécurité pour l'objet NTAuthCertificates, procédez comme suit :

1. Dans le champ **Ouvrir**, saisissez `adsiedit.msc`, puis appuyez sur **Entrée** ou cliquez sur **OK**.
2. Cliquez avec le bouton droit de la souris sur **Modification ADSI** et sélectionnez **Se connecter à**.
3. Dans la section **Point de connexion**, sélectionnez la valeur **Configuration** dans le champ Sélectionnez un **Contexte d'appellation connu**.
4. Double-cliquez sur **Configuration/Schéma** dans le volet de gauche.
5. Sélectionnez le dossier **CN=Configuration,DC=...** → **CN=Services** → **CN=Services de clés publiques** → **CN=NTAuthCertificates**.
6. Cliquez avec le bouton droit de la souris sur le dossier **CN=NTAuthCertificates**, sélectionnez **Propriétés** et ouvrez l'onglet **Sécurité**.
7. Cliquez sur le bouton **Avancé** et sélectionnez l'onglet **Audit**.
8. Cliquez sur la classe d'objet principal **Tout le monde**, cochez les cases **Propriétés en écriture**, **Supprimer**, **Modifier les permissions**, **Modifier le propriétaire**, **Toutes les écritures validées**, puis cliquez sur **OK**.

Vidéo d'intégration

Regardez la vidéo pour en savoir plus sur les principales fonctionnalités de la solution MDR.



Solution MDR. Vidéo d'intégration