

kaspersky

Programme d'assistance technique étendue pour Kaspersky Anti Targeted Attack

MSA pour KATA

1. Conditions générales

Voici une liste des cas de support technique pour lesquels Kaspersky fournira une assistance au propriétaire du certificat d'assistance technique étendue pour la plateforme Kaspersky Anti Targeted Attack (ici et après MSA pour KATA).

Ce programme d'assistance MSA pour KATA vise à fournir à l'Utilisateur final un support technique de meilleure qualité, par rapport aux conditions du support technique standard assuré conformément au Contrat de licence utilisateur final de Kaspersky, qui détermine les conditions d'utilisation du produit logiciel par l'Utilisateur final.

2. Définitions

L'expression « **Kaspersky CompanyAccount** » désigne le système de traitement en ligne des demandes de support technique de Kaspersky.

Le terme « **Produit(s)** » désigne le(s) produit(s) logiciel(s) de Kaspersky que le Client a acheté(s), déployé(s) et installé(s) conformément aux conditions d'un Contrat de licence conclu entre Kaspersky et le Client, et pour lequel (lesquels) le Client a conclu un Contrat de licence.

L'expression « **Utilisateur final** », « **Utilisateur** », « **Client** », (**Vous**) désigne une organisation qui dispose d'une licence opérationnelle pour le Produit et qui bénéficie d'un soutien conformément au présent Programme.

Le terme « **Incident** » désigne tout événement signalé par le Client, qui ne fait pas partie du fonctionnement standard d'un Produit et qui entraîne ou peut entraîner une interruption ou une réduction de la qualité du service fourni par le Produit.

L'expression « **Heure locale** » désigne le fuseau horaire du bureau local de Kaspersky.

Le terme « **Problème** » désigne une cause sous-jacente inconnue d'un ou de plusieurs incidents. Elle devient une erreur connue lorsque la cause première est connue et qu'une solution de contournement temporaire ou une alternative permanente a été identifiée.

L'expression « **Erreur connue** » désigne un Problème qui devient une Erreur connue lorsque la cause première est connue et qu'une solution de contournement temporaire ou une solution de remplacement permanente a été identifiée.

L'expression « **Erreur de produit** » désigne un comportement non déclaré du Produit.

L'expression « **Demande de service** » désigne une demande d'assistance, de livraison, d'information, de conseil ou de documentation émanant d'un Client, qui n'est pas liée à un mauvais fonctionnement ou à un dysfonctionnement du ou des Produits.

L'expression « **Attaque de virus** » désigne une situation de crise du Client, dans laquelle un virus non détecté par le ou les Produits dotés des bases antivirus et des modules exécutables les plus récents nuit à la continuité des activités et/ou à un grand nombre d'utilisateurs finals du Client. L'Attaque de virus est un incident lié à un produit.

L'expression « **Incident lié à une application malveillante / Incident lié à un virus** » signifie un incident non lié au produit, nécessitant que Kaspersky fournisse des recommandations sur la suppression d'applications malveillantes particulières, et/ou des descriptions d'applications malveillantes et/ou des outils spéciaux de suppression d'applications malveillantes.

L'expression « **Gravité/Urgence de l'incident** » désigne une mesure de la criticité d'un incident ou d'un problème pour l'entreprise, fondée sur les besoins de l'entreprise du Client. Pour en savoir plus, consultez l'annexe.

L'expression « **Temps de réponse** » désigne le temps écoulé entre la réception d'un incident et la réponse qualifiée à l'initiateur (via le système d'assistance, par email ou par téléphone).

L'expression « **Mise à jour** » désigne les bases de données antivirus émises par Kaspersky avec de nouvelles signatures de virus ou la modification des modules exécutables du Produit, qui améliorent ses performances et/ou étendent ses fonctionnalités.

L'expression « **Mise à niveau** » désigne une mise à jour du produit associée à l'attribution d'un nouveau numéro de version.

L'expression « **Solution de contournement** » désigne une procédure qui peut servir de solution temporaire à un incident.

L'expression « **Fausse alerte** », « **Faux positif** » désigne une situation dans laquelle le Produit détecte par erreur un fichier sûr comme étant infecté.

3. Description du programme d'assistance MSA pour KATA

Canaux de support technique :

- Portail Web du support technique de Kaspersky avec acceptation des demandes 24h/24, 365 jours par an
- Ligne téléphonique prioritaire, en fonction de l'urgence :
 - pour les demandes de niveau de gravité 1, 24h/24 et 365 jours par an ;
 - pour les demandes des niveaux de gravité 2 à 4, pendant les heures d'ouverture du bureau local de Kaspersky.
- Email (uniquement en cas de problème d'accès au portail Kaspersky CompanyAccount), prise en charge des demandes 24h/24, 365 jours par an

Traitement des incidents

Traitement des incidents via le portail Kaspersky CompanyAccount

Le système de traitement des demandes d'assistance technique Kaspersky basé sur le Web est disponible à l'adresse suivante : <https://companyaccount.kaspersky.com>

Ce système permet au client de bénéficier des services suivants :

- accès au compte personnel afin de créer, mettre à jour et suivre les incidents ;
- assistance technique et conseil en cas d'incidents pouvant survenir lors de l'installation, de la configuration et du fonctionnement du Produit ;
- signalement des détections de faux positifs du produit et demande de modification de la mise à jour des bases de données du produit afin d'assurer une détection appropriée.

Traitement des incidents par téléphone

Le support technique par téléphone est uniquement disponible pour les personnes de contact autorisées du Client.

Traitement des incidents par email

Le traitement des incidents par email peut être utilisé en cas de problèmes d'accès au portail web Kaspersky CompanyAccount. Il est accessible à toutes les personnes de contact autorisées du Client.

Temps de réponse

Kaspersky garantit les délais de réponse suivants, en fonction de l'urgence de la demande du client :

Niveau de gravité	Temps de réponse
Niveau 1	2 heures*
Niveau 2	6 heures ouvrées
Niveau 3	8 heures ouvrées
Niveau 4	10 ouvrées

* Un appel téléphonique est nécessaire en dehors des heures de bureau, y compris les week-ends et les jours fériés

Les demandes des clients du programme MSA pour KATA sont traitées avec une priorité plus élevée que les demandes de l'assistance standard.

Le niveau d'urgence est déterminé par la catégorie choisie par le client (à l'aide de la liste déroulante sur Kaspersky CompanyAccount) lorsqu'il a contacté le support technique et par la nature de l'incident. Kaspersky se réserve le droit de reconsidérer le niveau d'urgence de la demande si la gravité de la situation telle que définie par le client n'est pas validée. La liste des niveaux d'urgence et leurs descriptions figurent dans l'annexe.

Contrôle de résolution des incidents

À tout moment, un incident peut être soit du côté du Client (c'est-à-dire que le Client prend des mesures qui favoriseront/accéléreront la résolution du problème par Kaspersky), soit du côté de Kaspersky.

Un incident est du côté du Client lorsque Kaspersky demande des informations au Client. Lorsque le Client fournit les informations demandées à Kaspersky, l'incident est considéré comme étant du côté de Kaspersky. La période pendant laquelle l'incident peut être du côté du Client est limitée à 1 mois. En cas de réponse tardive du Client, l'incident est clôturé automatiquement.

Kaspersky est responsable uniquement pour la période pendant laquelle l'incident est de son côté.

Gestion de la qualité

Escalade des incidents et gestion des réclamations

Les réclamations concernant la qualité de l'assistance technique sont acceptées selon le principe suivant :

Niveau d'escalade	1	2
	Chef de l'équipe d'assistance, bureau régional de Kaspersky	Responsable commercial, bureau régional de Kaspersky

Le Client a la possibilité d'escalader un incident non résolu si Kaspersky en est responsable à ce stade.

Publication de la base de données antivirus à la demande du client en cas d'incident lié à une application malveillante ou de faux positif

En cas de faux négatif (lorsqu'un fichier infecté est identifié par le Produit comme sûr) ou, à l'inverse, de faux positif, à condition que les dernières bases de données anti-virus disponibles soient utilisées, le Client peut demander à ce que des modifications soient apportées aux signatures antivirus du Produit. Kaspersky fournit au Client les mises à jour du Produit qui assureront la détection correcte du fichier.

Kaspersky met en œuvre les services suivants :

- Traitement des demandes concernant la mise à disposition de bases de données antivirus (effectué par un groupe de spécialistes dédiés, en mode 24/7/365).
- Publication de mises à jour hautement prioritaires (accélérées) pour les abonnés au programme MSA pour KATA.
- Renseignement du client sur l'état d'avancement de ses demandes.

Conditions supplémentaires d'assistance

Le Client peut désigner jusqu'à 4 (quatre) personnes de contact autorisées à initier des demandes auprès du support technique de Kaspersky. Une liste de personnes de contact autorisées doit être définie dans le certificat Kaspersky MSA pour KATA. Pour modifier la liste des personnes de contact autorisées, le Client doit envoyer une demande écrite par l'intermédiaire Kaspersky CompanyAccount. Kaspersky fournira au Client une version actualisée du certificat Kaspersky MSA pour KATA.

Le Client peut enregistrer 36 incidents pendant la validité du certificat Kaspersky MSA pour KATA, sauf indication contraire dans les certificats valides.

Certains incidents peuvent nécessiter une reproduction du côté de Kaspersky afin de tester et de vérifier une infection virale ou une erreur du produit.

Le Client doit fournir à Kaspersky toutes les informations nécessaires et les logiciels ou matériels appropriés, qui peuvent être nécessaires pour reproduire les conditions dans lesquelles l'incident se reproduira et pourra être examiné. Cela peut s'avérer nécessaire si Kaspersky ne dispose pas du logiciel ou du matériel nécessaire.

Kaspersky s'efforcera de reproduire l'incident dès que toutes les informations et tous les logiciels et/ou matériels nécessaires auront été fournis.

Si l'incident n'a pas pu être reproduit, le client doit accorder aux spécialistes de Kaspersky un accès à distance supervisé au système défaillant.

Si l'incident ne peut être reproduit par aucune des parties, ou si le Client n'a pas donné accès à l'environnement réseau où l'incident pourrait être reproduit, ou bien s'il est détecté que la cause de l'incident se situe en dehors du Produit, l'incident ne peut être traité dans le cadre de ce Programme d'assistance.

Si le Client possède une licence Kaspersky Private Security Network (KPSN) ainsi que des licences Kaspersky Anti Targeted Attack, les conditions du programme MSA pour KATA s'appliqueront aux deux produits.

Limites du programme d'assistance technique étendue MSA pour KATA

L'assistance technique couverte par le programme MSA pour KATA ne sera pas mise en œuvre lors des incidents suivants :

- les incidents déjà résolus pour le Client (c'est-à-dire les incidents survenus sur une copie installée du Produit après que le même incident ait été résolu pour une autre copie du Produit) ;
- le dépannage de tous les problèmes similaires ou identiques à des problèmes déjà résolus (c'est-à-dire les incidents pour lesquels une solution précédemment produite peut être appliquée sans conseils supplémentaires de Kaspersky) ;
- les incidents causés par un dysfonctionnement du matériel du Client ;
- les incidents causés par l'incompatibilité des plateformes logicielles (y compris, mais sans s'y limiter, les logiciels bêta, les nouvelles versions de service packs ou d'ajouts, dont la compatibilité avec le Produit n'a pas été confirmée par Kaspersky) ;
- les incidents causés par l'installation et l'exécution d'applications tierces (y compris, mais sans s'y limiter, la liste des applications non prises en charge ou incompatibles publiée dans la documentation) ;
- les incidents pour lesquels le Client ne peut pas fournir d'informations exactes, comme le demande raisonnablement Kaspersky, afin de reproduire, d'enquêter et de résoudre l'incident ;
- les incidents qui surviennent à la suite d'une négligence ou d'une utilisation incorrecte des instructions de Kaspersky, qui, si elles avaient été correctement utilisées, auraient manifestement permis d'éviter l'incident.

Voici les types de demandes qui ne sont pas couverts par le programme MSA pour KATA (sans toutefois s'y limiter) :

- la vérification et la hiérarchisation des alertes de l'application KATA ;
- la réalisation d'enquêtes sur les incidents de sécurité (service disponible moyennant des frais supplémentaires) ;
- la résolution des incidents de sécurité.

4. Annexe

Niveaux de gravité des incidents liés aux Produits

« **Niveau de gravité 1** » (critique) désigne un problème grave lié au Produit, qui nuit à la continuité des activités du Client en interrompant le fonctionnement normal du Produit et qui provoque le plantage du ou des Produits ou du Système d'exploitation, ou qui entraîne une perte de données, le remplacement des paramètres par défaut par des valeurs non sécurisées ou des problèmes de sécurité, pour autant qu'il n'existe aucune solution de contournement.

La liste des incidents liés aux Produits, qui correspondent au niveau de gravité 1, comprend, sans s'y limiter, les problèmes suivants :

- tout le réseau local (ou sa partie critique) est inopérant, ce qui entrave ou suspend les processus de base de l'entreprise.

« **Niveau de gravité 2** » (élevé) désigne un problème modéré qui nuit à la fonctionnalité du produit mais n'entraîne pas de corruption ni de perte de données, ni de plantage du logiciel. Le niveau de gravité 1 est reclassé au niveau de gravité 2 lorsqu'une solution de contournement est disponible.

La liste des incidents liés aux Produits, qui correspondent au niveau de gravité 2, comprend, sans s'y limiter, les problèmes suivants :

- le produit fonctionne mal ou ne fonctionne pas, mais la continuité des processus commerciaux essentiels n'est pas interrompue.

« **Niveau de gravité 3** » (moyen) désigne un problème non critique ou une demande de service qui ne nuit pas à la fonctionnalité du Produit.

La liste des incidents qui correspondent au niveau de gravité 3, comprend, sans s'y limiter, les problèmes suivants :

- le produit est partiellement hors service (dysfonctionnements), mais les autres applications utilisées par le Client ne sont pas concernées.

« **Niveau de gravité 4** » (mineur) désigne d'autres problèmes ou demandes de service non critiques. Tous les incidents qui ne répondent à aucun des critères énumérés ci-dessus sont classés dans ce niveau de gravité.

Niveaux de gravité des incidents liés aux virus

« **Niveau de gravité 1** » (critique) désigne une attaque de virus qui compromet la continuité des activités du client en interrompant le fonctionnement normal du Produit et qui provoque le blocage du ou des Produits ou du ou des Systèmes d'exploitation, ou qui entraîne une perte de données, pour autant qu'il n'existe aucune solution de contournement.

La liste des incidents liés aux applications malveillantes, qui correspond au niveau de gravité 1, comprend, sans s'y limiter, les problèmes suivants :

- tout le réseau local (ou sa partie critique) est hors service ;
- une attaque de virus ;
- un faux positif pour les fichiers qui renvoient à des systèmes essentiels à l'activité de l'entreprise.

« **Niveau de gravité 2** » (élevé) désigne un problème modéré qui nuit à la fonctionnalité du produit mais n'entraîne pas de corruption ni de perte de données, ni de plantage du logiciel. Le niveau de gravité 1 est reclassé au niveau de gravité 2 lorsqu'une solution de contournement est disponible.

La liste des incidents liés aux applications malveillantes, qui correspond au niveau de gravité 2, comprend, sans s'y limiter, les problèmes suivants :

- l'infection de certains nœuds non critiques du réseau ;
- un faux positif pour les fichiers qui ne renvoient pas à des systèmes essentiels à l'activité de l'entreprise.

kaspersky

kaspersky

www.kaspersky.fr/
www.securelist.com

© 2022 AO Kaspersky Lab.
Tous droits réservés. Les autres noms et marques déposés appartiennent à leurs propriétaires respectifs