kaspersky

Programme d'assistance Technique Étendue Enterprise

MSA Enterprise

kaspersky

1. Conditions générales

Le présent document fournit une liste des cas d'assistance technique pour lesquels Kaspersky fournira une assistance au propriétaire du Certificat d'assistance technique étendue pour le niveau MSA Enterprise.

Ce programme d'assistance MSA Enterprise vise à fournir à l'Utilisateur final une assistance technique de meilleure qualité, par rapport à l'assistance technique standard effectuée conformément au Contrat de licence de l'utilisateur final Kaspersky, qui détermine les conditions d'utilisation du Produit logiciel par l'Utilisateur final.

2. Définitions

« Compte de l'entreprise » désigne le système de traitement des demandes de l'assistance technique Web Kaspersky.

« Produit(s) » désigne le ou les produits logiciels de Kaspersky que le Client a achetés, déployés et installés conformément aux conditions du Contrat de licence entre Kaspersky et le Client, et pour lesquels le Client a signé un Contrat de licence.

« Utilisateur final », **« Utilisateur »**, **« Client », (Vous/Votre)** désigne une organisation qui dispose d'une licence permettant d'utiliser le Produit pris en charge conformément à ce Programme.

« Incident » désigne tout événement signalé par le Client qui ne fait pas partie du fonctionnement normal d'un Produit et qui cause, ou peut causer, une interruption ou une réduction de la qualité du service fourni par le Produit.

« Heure locale » désigne le fuseau horaire du bureau local de Kaspersky.

« Problème » désigne la cause inconnue sous-jacente d'un ou de plusieurs Incidents. Un Problème devient une Erreur connue lorsque son origine est connue et qu'une solution de contournement temporaire ou permanente a été identifiée.

« Erreur connue » désigne un Problème qui devient une Erreur connue lorsque l'origine est connue et qu'une solution de contournement temporaire ou permanente a été identifiée.

« Erreur de produit » désigne un comportement non déclaré du Produit.

« Demande de service » désigne la demande d'un Client concernant l'assistance, la livraison, des informations, des conseils ou de la documentation, qui n'est pas liée à un mauvais fonctionnement ou au non-fonctionnement du ou des Produits.

« Épidémie de virus » désigne une situation de crise pour le Client lors de laquelle un virus non détecté par le ou les Produits disposant des dernières bases antivirus et des derniers modules exécutables affecte la continuité des activités et/ou de nombreux utilisateurs finaux du Client. Une Épidémie de virus est un Incident lié à un produit.

« Incident provoqué par un programme malveillant/virus » désigne un incident qui n'est pas lié au produit, nécessitant que Kaspersky formule des recommandations sur une suppression de programmes malveillants spécifique et/ou des descriptions de programmes malveillants, et/ou des outils de suppression de programmes malveillants spécifiques.

« Gravité/urgence de l'incident » désigne une mesure du caractère critique d'un incident sur les activités ou d'un problème relatif aux besoins commerciaux du Client. Voir l'Annexe pour en savoir plus.

« Temps de réponse » désigne le délai écoulé entre la réception du message faisant état de l'incident et la réponse qualifiée envoyée à la personne à l'origine du message (via le système d'assistance, par email ou par téléphone).

« Mise à jour » se réfère aux bases de données antivirus fournies par Kaspersky et comportant de nouvelles signatures de virus ou une modification des modules exécutables du Produit, et dont l'application améliore ses performances et/ou accroît sa fonctionnalité.

« Mise à niveau » désigne une mise à jour de Produit associée à l'attribution d'un nouveau numéro de version.

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

« Fausse alerte », **« Faux positif »** se rapporte à une situation au cours de laquelle le Produit désigne à tort un fichier sûr comme étant infecté.

3. Description du programme d'assistance MSA Enterprise

L'assistance technique, liée à l'utilisation des produits avec acceptation des demandes de maintenance après incident, est mise en œuvre comme suit :

- Portail Web d'assistance technique Kaspersky avec acceptation des demandes 24 h/24, 365 jours par an
- Ligne téléphonique prioritaire, en fonction de l'urgence :
    - pour les demandes de niveaux de gravité 1 et 2, 24 h/24, 365 jours par an ;
    - pour les demandes de niveaux de gravité 3 et 4, heures d'ouverture du bureau local de Kaspersky.
- Emails (uniquement en cas de problèmes d'accès au Compte de l'entreprise), acceptation des demandes 24 h/24, 365 jours par an
- Responsable de compte technique dédié, pendant les heures de travail, heure locale

Traitement des incidents

Traitement des incidents via le portail Web du Compte de l'entreprise

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

Le Client peut, par l'intermédiaire de ce système, profiter des avantages suivants :

- accès à son compte personnel afin de créer, de mettre à jour et de surveiller les incidents ;
- assistance technique et conseils à propos des incidents qui peuvent se produire lors de l'installation, de la configuration et du fonctionnement du Produit ;
- assistance technique concernant la désinfection des fichiers altérés par des programmes malveillants et la suppression de programmes malveillants des ordinateurs du Client protégés par le Produit et ses dernières bases de données antivirus.

Traitement des incidents par téléphone

L'assistance technique par téléphone est disponible uniquement pour les contacts autorisés du Client.

Temps de réponse

Kaspersky garantit les temps de réponse indiqués ci-dessous, en fonction de l'urgence de la demande du Client :

Niveau de gravité	Temps de réponse
Niveau 1	30 minutes*
Niveau 2	4 heures*
Niveau 3	6 heures ouvrées
Niveau 4	8 heures ouvrées

*Appel téléphonique requis en dehors des heures de travail, week-ends et jours fériés inclus

Les demandes formulées par les clients de MSA Enterprise reçoivent la plus haute priorité par rapport aux demandes soumises dans le cadre du package d'assistance standard.

Le niveau d'urgence est déterminé par la catégorie choisie par le client (via la liste déroulante dans le Compte de l'entreprise) lorsqu'il contacte l'assistance technique et par les grandes lignes de l'incident. Kaspersky se réserve le droit de modifier le niveau d'urgence de la demande si la gravité du cas spécifié par le client n'est pas confirmée. La liste des niveaux d'urgence, ainsi que leurs descriptions, est fournie dans l'Annexe.

Contrôle de la résolution des incidents

À tout moment, un incident peut survenir soit du côté Client (le Client prend des mesures pour appuyer et accélérer la résolution du problème par Kaspersky) soit du côté de Kaspersky.

Un incident survient côté Client lorsque Kaspersky demande des informations auprès du Client. Lorsque le Client fournit à Kaspersky les informations demandées, on considère que l'incident survient du côté de Kaspersky. La période au cours de laquelle l'incident peut rester côté Client est limitée à 1 mois. Dans le cas où la réponse du Client est tardive, l'incident est clos après expiration du délai.

Kaspersky est uniquement responsable pendant la période au cours de laquelle l'incident se trouve de son côté.

Un responsable de compte technique dédié (TAM) est assigné par Kaspersky dans le but de maintenir une voie de communication intégrée avec le client.

Le TAM est un salarié de Kaspersky et gère le traitement de tous les incidents du client. Les responsabilités du responsable de compte technique sont déterminées comme suit :

- il organise les communications pour le traitement des incidents par les équipes techniques de Kaspersky;
- il avise le Client de l'état actuel des incidents en lui fournissant des rapports trimestriels ;
- il supervise l'état d'avancement des tâches relatives aux demandes du Client et met en place des remontées opportunes lors du traitement des demandes ;
- il apporte son soutien au département informatique du Client conformément aux recommandations et instructions fournies par les spécialistes Kaspersky;
- il coopère de façon analytique avec le Client afin de résoudre les incidents techniques et opérationnels en cours.

Le TAM est joignable pendant les heures de travail, du lundi au vendredi de 09 h 00 à 18 h 00. * heure locale par téléphone fixe, par téléphone cellulaire et par email. Si le TAM est indisponible (en dehors des heures normales de travail, y compris les week-ends) les demandes du Client sont dirigées vers le manager en service sur la ligne d'assistance technique MSA.

Les heures de travail peuvent varier selon la région. Consultez votre certificat de maintenance Kaspersky pour en savoir plus.

Le Client désigne des personnes à contacter (conformément aux conditions d'assistance supplémentaires) pour les communications avec Kaspersky, et partage avec ces derniers ses coordonnées (email, numéro de téléphone et autres renseignements le cas échéant) pour garantir la cohérence et l'efficacité de la collaboration dans le cadre de la résolution des incidents.

Gestion de la qualité

Remontée des incidents et gestion des réclamations

Les réclamations concernant la qualité de l'assistance technique sont acceptées conformément au schéma suivant :

Niveau	1	2	3
	TAM	Chef de l'équipe d'assistance, bureau régional de Kaspersky	Responsable commercial des affaires (contact professionnel)

Le Client peut faire remonter des incidents non résolus s'ils se trouvent du côté de Kaspersky.

Mise à disposition de rapports sur les incidents ouverts

Pendant le processus de résolution des incidents, Kaspersky mettra tout en œuvre pour fournir rapidement au Client des informations sur le statut des incidents ouverts, comme indiqué dans le tableau suivant.

Niveau de gravité	Calendrier des rapports
Niveau 1	En vertu d'un accord, mais pas plus souvent qu'une fois par jour (par email ou par téléphone)
Niveau 2	Dans le cadre des rapports réguliers
Niveau 3	
Niveau 4	

Publication de la base de données antivirus suite à une demande du client concernant des incidents impliquant un programme malveillant ou des faux positifs

En cas de faux négatif (lorsqu'un fichier infecté est identifié par le Produit comme sûr) ou, au contraire, de faux positif, et à condition que les bases de données antivirus les plus récentes soient utilisées, le Client peut demander à ce que des modifications soient apportées aux signatures antivirus du Produit. Kaspersky fournit au Client la mise à jour du Produit qui assurera la bonne détection du fichier.

Kaspersky met en œuvre les activités suivantes :

- Traitement des demandes concernant la publication des bases de données antivirus (effectué par un groupe de spécialistes dédiés 24 h/24, 7 j/7 et 365 j/an)
- Publication des mises à jour de haute priorité (accélérée) pour les abonnés de MSA Enterprise.
- Communication avec le Client pour l'informer de l'avancement de ses demandes par le biais du responsable de compte technique.

Mise à disposition de correctifs publics et privés

- Traitement des demandes concernant la publication de correctifs publics et privés (effectué par un groupe d'ingénieurs dédiés pour les demandes des abonnés Enterprise)
- Communication avec le Client pour l'informer de l'avancement de ses demandes par le biais du responsable de compte technique

Kaspersky mettra en place tous les efforts commercialement raisonnables pour publier un code de correction du programme privé (correctif privé). Les codes de correction de programme sont publiés en fonction de la répartition du cycle de vie de l'assistance du produit, conformément aux Conditions générales du service d'assistance (une version à jour est disponible à l'adresse suivante : https://support.kaspersky.com/support/rules#fr_fr).

Les conditions d'utilisation des corrections du programme privé sont soumises au Contrat de licence signé entre Kaspersky et le Client.

Service de bilan de santé (Health Check)

Le client ayant souscrit à un contrat d'assistance technique étendue, bénéficie une fois par an d'un service de bilan de santé sur la durée du contrat. Le service bilan de santé propose un audit des paramètres des produits Kaspersky afin de déterminer s'ils répondent aux bonnes pratiques et recommandations de Kaspersky. Comme livrable, le client recevra une liste de contrôle avec les conclusions et les recommandations fournies par le responsable de compte technique. Le service est délivré à distance et dure 1 (un) jour ouvrable. La date et les conditions de livraison devront être convenues au moins deux semaines à l'avance.

Conditions supplémentaires d'assistance

Le Client peut désigner jusqu'à 8 (huit) contacts autorisés à initier des demandes auprès de l'assistance technique de Kaspersky. Une liste des contacts autorisés doit être définie sur le certificat Kaspersky MSA Enterprise. Pour modifier la liste des contacts autorisés, le Client doit envoyer une demande écrite via le Compte de l'entreprise. Kaspersky fournira au Client une version mise à jour du certificat Kaspersky MSA Enterprise.

Le Client peut enregistrer un nombre illimité d'incidents au cours de la durée de validité du certificat Kaspersky MSA Enterprise.

Certains incidents peuvent exiger une reproduction côté Kaspersky afin de tester et de vérifier une infection par virus ou une erreur de produit.

Le Client doit fournir à Kaspersky toutes les informations nécessaires ainsi que les logiciels ou le matériel spécifique(s) pouvant être requis pour reproduire les conditions dans lesquelles l'incident se reproduira à des fins d'examen. Cette étape peut s'avérer nécessaire si Kaspersky ne dispose pas des logiciels ou du matériel requis.

Kaspersky s'efforcera de reproduire l'incident une fois l'ensemble des informations, des logiciels et/ou du matériel nécessaire fournis.

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

Si l'incident ne peut pas être reproduit par l'une ou l'autre partie, ou si le Client n'a pas accordé l'accès à l'environnement réseau au sein duquel l'incident pourrait être reproduit, ou si l'on détecte que la cause de l'incident va au-delà du Produit lui-même, l'incident ne peut pas être classé dans le cadre de ce programme d'assistance.

Limitations du programme d'assistance technique étendue MSA Enterprise

L'assistance technique couverte par le programme MSA Enterprise ne doit pas être mise en œuvre dans les situations suivantes :

- incidents déjà résolus pour le Client (c'est-à-dire, un incident survenu sur une copie installée du Produit après que le même incident a été résolu pour une autre copie du Produit) ;
- résolution de tout problème similaire ou identique à un problème qui a déjà été résolu (c'est-à-dire, les incidents pour lesquels une solution fournie auparavant peut être appliquée sans l'intervention de Kaspersky) ;
- incidents causés par un dysfonctionnement du matériel du Client ;
- incidents causés par l'incompatibilité de la plateforme logicielle (y compris, mais sans s'y limiter, les logiciels bêta, les nouvelles versions des Service Packs ou des ajouts, dont la compatibilité avec le Produit n'a pas été confirmée par Kaspersky) ;
- incidents causés par l'installation et l'exécution d'applications tierces (figurant notamment, mais sans s'y limiter, sur la liste des applications non prises en charge ou incompatibles publiée dans la documentation) ;
- incidents pour lesquels le Client ne peut pas fournir des informations précises, à la demande

raisonnable de Kaspersky, afin de reproduire, d'étudier et de résoudre l'incident ;

- incidents survenus suite à une négligence ou à une mauvaise utilisation des instructions de Kaspersky qui, si elles avaient été suivies, auraient de toute évidence permis d'éviter l'incident.

4. Annexe

Niveaux de gravité des incidents de produit

« Niveau de gravité 1 » (critique) désigne un problème critique du Produit qui affecte la continuité des activités du Client par des interruptions dans le fonctionnement normal du Produit et qui entraîne le plantage du ou des Produits ou du système d'exploitation, une perte de données, le remplacement des paramètres par défaut par des valeurs non sécurisées ou des problèmes de sécurité, à condition qu'aucune solution de contournement ne soit disponible.

La liste des incidents liés à un Produit qui se réfèrent au niveau de gravité 1 inclut, mais sans s'y limiter, les problèmes suivants :

- l'ensemble du réseau local (ou sa partie critique) est inopérant(e), ce qui entrave ou suspend les processus opérationnels de base.

« Niveau de gravité 2 » (élevé) désigne un problème modéré qui affecte la fonctionnalité du produit, mais ne cause pas la corruption/la perte de données ou le plantage du logiciel. Le niveau de gravité 1 est reclassé en niveau de gravité 2 lorsqu'une solution de contournement est disponible.

La liste des incidents liés à un Produit qui se réfèrent au niveau de gravité 2 inclut, mais sans s'y limiter, les problèmes suivants :

- le produit ne fonctionne pas correctement ou ne fonctionne pas du tout, mais la continuité des processus de base de l'entreprise n'est pas entravée.

« Niveau de gravité 3 » (moyen) désigne un problème ou une demande de service non critique qui n'affecte pas la fonctionnalité du Produit.

La liste des incidents qui se réfèrent au niveau de gravité 3 inclut, mais sans s'y limiter, les problèmes suivants :

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

« Niveau de gravité 4 » (mineur) désigne les autres problèmes ou demandes de service non critiques. Reportez-vous à ce niveau de gravité pour tous les incidents qui ne remplissent pas les critères susmentionnés.

Niveaux de gravité des incidents liés à un virus

« Niveau de gravité 1 » (critique) désigne une épidémie de virus qui affecte la continuité des activités du Client par des interruptions dans le fonctionnement normal du Produit et qui entraîne le plantage du ou des Produits ou du ou des systèmes d'exploitation, ou une perte de données, à condition qu'aucune solution de contournement ne soit disponible.

La liste des incidents liés à un programme malveillant qui se réfèrent au niveau de gravité 1 inclut, mais sans s'y limiter, les problèmes suivants :

- l'ensemble du réseau local (ou sa partie critique) est inopérant(e) ;
- épidémie de virus ;
- faux positifs concernant les fichiers qui se réfèrent à des systèmes essentiels à l'entreprise.

« Niveau de gravité 2 » (élevé) désigne un problème modéré qui affecte la fonctionnalité du produit, mais ne cause pas la corruption/la perte de données ou le plantage du logiciel. Le niveau de gravité 1 est reclassé en niveau de gravité 2 lorsqu'une solution de contournement est disponible.

La liste des incidents liés à un programme malveillant qui se réfèrent au niveau de gravité 2 inclut, mais sans s'y limiter, les problèmes suivants :

- infection de certains nœuds de réseau non critiques ;
- faux positifs concernant les fichiers qui ne se réfèrent pas à des systèmes essentiels à l'entreprise.

www.kaspersky.com
www.securelist.com