

Cegid eConnect

Prérequis techniques

À propos de ce document

Ce document décrit les prérequis techniques associés au service Cegid eConnect en mode SaaS (Software as a Service) éditées, hébergées et exploitées par Cegid.

Ce document couvre les prérequis techniques relatifs aux postes de travail, aux aspects réseau et télécommunication ainsi qu'aux périphériques. Le respect de ces prérequis est essentiel au bon fonctionnement de ces solutions. La responsabilité de Cegid ne pourra être engagée en cas de dysfonctionnement de la solution lié à leur non-respect. Dans le cas d'une utilisation d'autres solutions Cegid, le Client doit s'assurer de respecter les recommandations communes à l'ensemble de l'offre proposée. Pour un conseil personnalisé, contactez votre Ingénieur Commercial. Si les utilisateurs sont répartis sur des sites géographiques distincts, il appartient au client de vérifier les tests de latences depuis chacun des sites utilisateurs recensés.

Il est à destination des équipes techniques client (réseau, sécurité, DSI) et définit les règles à mettre en œuvre sur les équipements proxy / firewall / reverse-proxy / WAF afin de sécuriser et autoriser les flux nécessaires entre leur installation On-Premise et la plateforme Cegid.

Mentions légales

La permission est accordée en vertu du présent Accord pour télécharger les documents détenus par Cegid et pour utiliser l'information contenue dans les documents uniquement en interne, à condition que: (a) la mention de copyright sur les documents demeure sur toutes les copies du matériel ; (b) l'utilisation de ces documents soit à usage personnel et non commercial, à moins qu'il n'ait été clairement défini par Cegid que certaines spécifications puissent être utilisées à des fins commerciales ; (c) les documents ne seront ni copiés sur des ordinateurs en réseau, ni publiés sur quelque type de support, à moins d'en avoir obtenu l'autorisation explicite de Cegid; et (d) aucune modification ne soit apportée à ces documents.

Sommaire

À propos de ce document.....	2
Mentions légales.....	2
Sommaire.....	3
Généralités et recommandations	4
Recommandations sur les flux Internet	4
Recommandations sur le réseau local	4
Recommandations sur le dimensionnement des accès Télécom	4
Recommandation sur la latence	5
Notes Importantes	5
Flux réseaux sortants vers Cegid eConnect	6
Flux réseaux entrants depuis Cegid eConnect	7
Adresses IP publiques d'appel depuis Cegid eConnect	7
URL à exposer.....	7
Exigences de sécurité - Authentification par Header (Obligatoire)	7
Exigences de sécurité – Validation des types d'échanges	7
Recommandations d'architecture sécurisée	8
Filtrage par domaine (FQDN) et Inspection TLS pour les flux sortants	8
Utiliser un reverse-proxy.....	8
Logs obligatoires Journaliser.....	8
Durcissement TLS.....	8

Généralités et recommandations

Le service **Cegid eConnect** est entièrement hébergée et exploitée par Cegid. Les Clients accèdent au service eConnect au travers d'une infrastructure Télécom mise en place par leurs soins en adéquation avec les recommandations techniques de Cegid décrites dans les paragraphes suivants.

Les modes de connexion possibles et les accès Télécom supportés en standard sont fonction de chaque solution On Demand. Il convient néanmoins de noter les points suivants :

- La mise en place de certains accès Télécom pourra être sujet à devis et nécessiter une étude technique.
- Toute demande de connexion et d'accès à la plateforme d'hébergement non standard devra être transmise à Cegid pour étude et validation. Cegid se réserve le droit de refuser la demande ou de la soumettre à devis.

Recommandations sur les flux Internet

- L'utilisation en mobilité (type réseau 3G ou satellite) n'est pas adaptée et n'est pas validée pour la solution Cegid eConnect.
- Privilégier les accès haut-débit SDSL ou fibre, de qualité et adaptés à l'ensemble de vos usages (SaaS et autres usages).
- Mettre en œuvre une solution de priorisation des flux vers le Cloud Cegid et de visibilité des flux (telle que Cegid Cloud Access Box).
- Le Client pourra, s'il le désire, ou si le profil d'utilisation de sa ligne en dehors des flux interactifs avec la solution Cegid eConnect le justifie, dédier une ligne Internet pour l'utilisation exclusive de sa solution Cegid eConnect répondant aux prérequis techniques fournis dans ce document.

Recommandations sur le réseau local

- Privilégier les connexions filaires Ethernet ainsi qu'un câblage et des équipements réseaux performants (switch gérables récents).
- Éviter les connexions en Wifi car elles peuvent engendrer des latences élevées aléatoires.

Recommandations sur le dimensionnement des accès Télécom

Le dimensionnement de vos accès à vos solutions Cegid dépend de plusieurs critères :

- Les préconisations spécifiques à chaque solution et fournies par Cegid
- L'utilisation de votre solution SaaS
- Les utilisations annexes de votre accès Internet en dehors de votre solution SaaS (surf, Messagerie etc...)

Les indications fournies ne constituent pas un engagement de la part de Cegid car elles dépendent de vos usages et de la qualité de la liaison fournie par votre opérateur. Les indications fournies au paragraphe «

Dimensionnement des accès Télécom » concernent uniquement les usages interactifs liés à vos applications Cegid. Elles ne tiennent pas compte des autres flux :

- Flux SaaS consommateurs de bande passante tels que les flux d'impression, les flux de numérisation de documents,
- Flux liés à des mises à jour de vos applications métiers.
- Flux Internet

Vous devez vous assurer de ne pas perturber vos flux SaaS par d'autres autres usages liés à Internet tels que :

- Mises à jour système,
- Mises à jour logiciels,
- Mises à jour antivirus,
- Flux audio ou vidéo,
- Autres flux « récréatifs »,
- Interconnexion de vos sites.

Recommandation sur la latence

La latence mesure en ms (millisecondes) le temps aller-retour entre le poste d'un utilisateur et le Cloud Cegid. Les flux interactifs à destination du Cloud Cegid doivent avant tout bénéficier d'une latence faible et surtout ne pas être perturbés par d'autres flux tels que des mises à jour (système, antivirus ou logiciel), des échanges de fichiers volumineux, des flux audio ou vidéo, ou tout autre flux « récréatif ». La latence peut varier fortement en fonction de l'utilisation de la liaison Télécom.

Notes Importantes

- Dès lors que la capacité de la liaison approche de la saturation, des pics de latence peuvent apparaître.
- Il peut être nécessaire de redimensionner la liaison Télécom ou bien de prioriser les flux à destination du Cloud Cegid.
- Les préconisations sont valides uniquement dans le cadre de sessions interactives avec l'application en ligne Cegid eConnect.
- Ces préconisations ne prennent pas en compte les besoins en bande passante nécessaires à l'exécution d'autres applications que Cegid eConnect, à l'échange d'informations avec d'autres applications du Système d'Information ou avec la plateforme (type échange de fichiers ou téléchargement de documents) et au support des autres types de flux Internet du Client comme la navigation Internet ou la messagerie...
- La responsabilité de Cegid ne pourra être engagée en cas de non-respect par le Client des prérequis techniques fournis dans ce document.

Flux réseaux sortants vers Cegid eConnect

Usage	Environnement	Domaine
Gestion API Keys		accounts.cegid.com
Auth Run (OAuth2)		oauth.cegid.com
API eFacture	Production	api-efacture.cegid.cloud
Storage Azure	Production	OutgoingInvoices-efacture.cegid.cloud PAInvoices-efacture.cegid.cloud
API eFacture	SandBox	sboxapi-efacture.cegid.cloud
Storage Azure	SandBox	SDBXOutgoingInvoices-efacture.cegid.cloud SDBXPAInvoices-efacture.cegid.cloud

Ces flux sont uniquement en HTTPS 443.

Flux réseaux entrants depuis Cegid eConnect

Ces flux nécessitent une exposition publique de votre produit Cegid OnPremise pour recevoir les évènements.

Adresses IP publiques d'appel depuis Cegid eConnect

Environnement	IP
SandBox	20.40.131.128
Production	20.40.131.128

L'ensemble des communications depuis Cegid eConnect vers vos infrastructures On-Premise sera initiée depuis ces adresses IP publiques. Elles doivent être toujours autorisés pour permettre la communication avec Cegid eConnect.

URL à exposer

En fonction du produit Cegid intégré à eConnect, plusieurs URL seront à exposer de façon sécurisée. Veuillez-vous référer à la documentation spécifique à votre produit Cegid.

Exigences de sécurité - Authentification par Header (Obligatoire)

En fonction du produit Cegid intégré à eConnect, nous vous recommandons de filtrer les échanges par authentification des en-têtes. Veuillez-vous référer à la documentation spécifique à votre produit Cegid.

Exigences de sécurité – Validation des types d'échanges

En fonction du produit Cegid intégré à eConnect, nous vous recommandons de filtrer les types échanges. Veuillez-vous référer à la documentation spécifique à votre produit Cegid.

Recommandations d'architecture sécurisée

Filtrage par domaine (FQDN) et Inspection TLS pour les flux sortants

Les firewalls nouvelle génération (Palo Alto, Fortinet, CheckPoint, Stormshield, Cisco FTD, etc.) permettent :

- Filtrage sortant sur FQDN (DNS Based Filtering)
- Inspection TLS permettant d'interpréter le champ SNI
- Définition d'ACL par regex d'URL C'est la méthode officiellement recommandée pour les services cloud dynamiques.

Utiliser un reverse-proxy

Avantages :

- Cloisonnement du serveur OnPremise
- Journaux centralisés
- Réécriture d'URL si besoin
- Absorption des preflight OPTIONS
- Protection DDoS / WAF

Exemples : NGINX / Apache / F5 / FortiWeb / Azure FrontDoor...

Logs obligatoires Journaliser

- Toutes les tentatives POST/OPTIONS
- Présence du header API key
- Code retour Produit Cegid OnPremise
- Timestamps et IP source7

Durcissement TLS

- TLS1.2 minimum
- Interdire TLS1.0 / 1.1
- Cipher suites modernes