

Conditions Spécifiques

ARTICLE 1 : Définitions

Tous les termes commençant par une majuscule et non définis dans les présentes Conditions Spécifiques auront, sauf précision explicite contraire, le sens qui leur est donné dans les Conditions Générales de Vente.

ARTICLE 2 : Objet

Les présentes Conditions Spécifiques ont pour objet de préciser les conditions applicables à la fourniture par CELESTE à ses Clients des Services : « UTM », « Protection Antivirus IPS » et « Services Managés »

ARTICLE 3 : UTM

CELESTE propose, dans le cadre de la vente de ses Connexions, un service appelé UTM. Celui-ci peut être fourni sur un équipement présent sur le Site Client ou sur un outil de sécurité centralisé hébergé dans les datacenters de CELESTE, et mutualisé entre plusieurs clients.

Le Matériel mis à disposition du Client appartient à CELESTE et doit être restitué à la fin de Contrat.

ARTICLE 4 : Filtrage / Antivirus / IPS

CELESTE propose un filtrage des flux antivirus et un outil de prévention des intrusions. L'activation de la fonctionnalité de protection antivirus IPS n'est autorisée que selon les protocoles suivants : ports FTP, HTTP, IMAP, POP3, SMTP, FTPS, HTTPS, IMAPS, POP3S, SMTPS en activant le déchiffrement SSL.

Le filtrage est réalisé sur les flux web transitant par la connexion CELESTE, sur les flux ci-dessus. Les autres protocoles ne sont pas filtrés. De même, certains fichiers compressés ne peuvent être filtrés. CELESTE ne réalise aucun filtrage antivirus sur les postes de travail du Client.

CELESTE informe le Client que le filtrage Antivirus des flux constitue une première protection, mais qu'il ne saurait se substituer à un logiciel antivirus installé et mis à jour sur chacun des postes de travail du Client.

CELESTE informe le Client que l'outil IPS (prévention des intrusions) fournit une protection vis à vis des intrusions d'un tiers sur les ordinateurs reliés au réseau local du Client. Toutefois, une attaque malveillante peut franchir cette protection. CELESTE recommande aux Clients qui hébergent des données sensibles de prendre des protections supplémentaires. CELESTE ne peut en aucun cas être tenue pour responsable des dommages causés par l'intrusion de tiers dans le réseau local du Client par le biais du réseau Internet.

L'outil IPS est configuré uniquement pour les sessions ouvertes par des postes de travail vers Internet, et non pour la protection de serveurs depuis Internet.

Le service Antivirus/IPS est standard, et ne peut être personnalisé pour le Client.

ARTICLE 5 : Services managés

Les services managés désignent l'ensemble des services réalisés par CELESTE sur l'UTM du Client. Ces prestations comprennent la gestion, la configuration et l'optimisation des produits souscrits par le Client.

Lorsque le Client souscrit à des « Services managés », il bénéficie d'un des 2 niveaux de services suivants :

Services managés	Essentiels	Premium
Mode de management	Self managé	Full managé
Maintenance matérielle	✓	✓
Mises à jour de sécurité		✓
Active Directory / SSO		✓
Nomade Ipsec		✓
Règles SD-WAN (IPsec/VPN) - Sous-couche / Surcouche*		✓
Règles de routage et optimisation des chemins*		✓
Configuration IPS / AV		✓
Filtrage DNS / Filtrage Web / Filtrage applicatif		✓
Configuration des éléments réseaux		✓

Servies managés « Essentiels » : ce niveau de service inclut uniquement la mise à disposition d'un matériel UTM fonctionnel ainsi que sa maintenance, c'est-à-dire son remplacement en cas de défaut ou de panne.

Les mises à jour de sécurité ainsi que toute modification de configuration ne sont pas incluses. Cependant, des modifications de configuration peuvent être réalisées par CELESTE à la demande du Client. Elles seront facturées selon la grille tarifaire des prestations d'assistance technique (Volet E du Contrat).

Servies managés « Premium » : ce niveau de service offre au Client une gestion complète de son UTM et des configurations sur demande.

Le Client peut demander autant de configurations de l'UTM qu'il le souhaite dans le cadre du périmètre limitativement défini ci-dessous :

- Ajout/Suppression/Modification firewall et sécurité policy
- Ajout/Suppression/Modification utilisateur/groupe utilisateur
- Ajout/Suppression/Modification objet

Dans le cas où le Client souhaite manager lui-même son UTM, CELESTE peut lui fournir les accès aux configurations du Service (et notamment les règles de sécurité et de filtrage web). Le Client s'engage alors à signer une décharge de responsabilité et à donner l'accès aux configurations à du personnel qualifié de son organisation.

Dans ce cas de figure, le Client est le seul responsable de la configuration du Service et de sa gestion. En cas de panne sur l'accès Internet ou sur le réseau du Client, ou en cas de défaut de sécurité liés à une erreur de configuration, CELESTE décline toute responsabilité.

Les éventuelles Interruptions de service dans ce cas ne pourront donner lieu au versement de pénalités. En cas de demande du Client d'une intervention d'urgence sur la configuration de l'UTM, CELESTE facturera cette prestation au tarif figurant dans la grille tarifaire des prestations d'assistance technique (Volet E du Contrat).

ARTICLE 6 : Configuration initiale

CELESTE réalise une configuration "simple" de l'UTM du Client dans la limite de 4 VLANs, 2 VPN, 50 Policies. Pour toute demande nécessitant une configuration plus complexe, le Client doit souscrire à l'option "UTM: Configuration complexe". En cas de souscription à cette option, CELESTE fournit au Client un formulaire de collecte d'information. Le Client devra le retourner sous un délai maximal de 5 jours ouvrés. Au-delà, le Client se verra appliquer sur son UTM une configuration dite « simple ».

ARTICLE 7 : Modifications de configuration

Le Client peut effectuer des demandes de modifications de configuration sur son UTM. Une demande équivaut à un mail et un domaine de configuration et son traitement ne peut excéder un temps de configuration égal à 30 minutes.

Si les demandes effectuées par le Client dépassent le forfait souscrit en termes d'actes et de temps alloué, alors les demandes supplémentaires seront facturées au tarif figurant dans la grille tarifaire des prestations d'assistance technique (Volet E du Contrat).

Toute demande de changement de configuration devra être effectuée par e-mail à l'adresse support@celeste.fr ou via l'espace client <https://espace-clients.celeste.fr/>.

La demande sera traitée par CELESTE sous 2 jours ouvrés. Les modifications de configurations sont par défaut réalisées en heures ouvrées, c'est-à-dire du lundi au vendredi de 8h30 à 18h30, heure de Paris, sauf jours fériés.

Si le Client souhaite que sa modification de configuration soit réalisée en dehors des heures ouvrées indiquées ci-dessus, il devra adresser sa demande à CELESTE en respectant un délai de prévenance de 14 jours.

Les modifications de configuration effectuées en heures non ouvrées seront facturées au tarif figurant dans la grille tarifaire des prestations d'assistance technique (Volet E du Contrat).

ARTICLE 8 : Mises à jour logicielles

Dans le cadre des Services managés « premium », CELESTE s'engage à appliquer les dernières mises à jour de sécurité publiées par l'éditeur de la solution dans les meilleurs délais à compter de leur publication à condition qu'elles n'entraînent pas une régression du service.

L'éditeur de la solution déploie des efforts dans une limite raisonnable afin d'apporter des solutions aux menaces sur Internet. Ces solutions sont développées en réponse à l'évolution de l'activité sur Internet.

ARTICLE 9 : Attaques de déni de service

CELESTE informe le Client que le Service n'est pas un outil de protection contre les attaques de déni de service (DDOS).

Conditions Spécifiques

ARTICLE 10 : Confidentialité

Le Client pourra être destinataire de certaines informations, notamment (liste non exhaustive) les mises à jour logicielles, les mises à jour de sécurité, les évolutions fonctionnelles, ainsi que d'autres informations commerciales ou techniques concernant le Service. Pendant toute la durée du Contrat augmentée d'une période de deux (2) ans après son terme pour laquelle que cause que ce soit, le Client s'engage à ne pas divulguer ces informations à des tiers sans l'accord préalable et écrit de CELESTE.

ARTICLE 11 : Limitations du Service

Les offres de Liens d'Accès incluant les Services sont adaptées au débit de l'offre dans le cadre d'un usage normal. En cas de besoins spécifiques de paramétrage ou d'une utilisation accrue des Services, CELESTE pourra proposer au Client une mise à niveau de la solution nécessitant une modification de la tarification du Service. Si le Client refuse cette recommandation, CELESTE ne pourra être tenue pour responsable de toute dégradation du Service liée au sous-dimensionnement de l'Équipement.

Concernant le Service « UTM », CELESTE recommande une limitation d'utilisateurs simultanés par modèle d'équipement selon les modalités suivantes :

Modèle d'équipement	Nombre d'utilisateurs simultanés maximum recommandé
Fortigate 50G	50
Fortigate 90G	90
Fortigate 120G	120
Fortigate 200G	200
Fortigate 400F	500

matériel similaire à celui initialement prévu en cas d'indisponibilité ou de fin de vie du matériel.

ARTICLE 12 : Authentification des utilisateurs

Si le Client dispose d'une authentification des utilisateurs par Active Directory, et qu'il a souscrit à l'option « Configuration Active Directory », alors le Service utilisera ce système d'authentification.

Dans les autres cas de figure, l'authentification sera réalisée par une liste fixe d'utilisateurs.

Lors de la configuration du Service, si celle-ci est réalisée par CELESTE, le Client transmettra à CELESTE la liste des utilisateurs.

Par la suite, toutes les modifications de cette liste seront considérées comme des modifications de configurations détaillées à l'article 7 « Modifications de Configuration » des présentes Conditions Spécifiques.

ARTICLE 13 : Accès distants

Les accès distants fournis dans le cadre du Service sont utilisables sur des postes de travail suivants :

VPN IPsec pour accueil de stations nomades et points à points. Compatible Cisco, Windows, MacOS, IOS (Ipad, iPhone), Android.

VPN SSL Tunnel pour accueil de solutions nomades. Compatible Windows, MacOS, Linux, Android - Incompatible IOS.

Cartes Token de sécurité (code d'accès changeant). Compatible en IPsec/SSL avec Windows, MacOS, Android, et en SSL avec Linux.

Selon le modèle d'Équipement, CELESTE ne pourra dépasser la quantité maximum d'accès VPN Ipsec et SSL alloués préconisée par l'éditeur.

ARTICLE 14 : Responsabilité

En cas de défauts causés à l'UTM du fait d'une utilisation inappropriée ou anormale de la part du Client ou de l'utilisateur final, d'un entretien inadéquat, d'une réparation ou d'une modification des produits et/ou du logiciel intégré non autorisée par CELESTE, le Client sera facturé des frais du Matériel détaillés au Volet E du présent Contrat.

Date, signature et cachet