

UCOPIA pour l'entreprise, de la PME au Grand Compte.



- Connexions internet pour les employés et les visiteurs (sous-traitants, partenaires)
- Sécurité et gestion des accès Wi-Fi et/ou filaire
- Politiques d'accès aux applications dépendantes du profil et du contexte (lieu, heure,...)
- Mise en conformité avec la loi contre le terrorisme 2006 et conservation des données de connexion
- Simplicité et confort d'utilisation

➤ L'accès internet pour le visiteur et pour l'employé

Les employés et les visiteurs de l'entreprise veulent se connecter à Internet et au système d'information partout dans et à l'extérieur de l'entreprise. Selon NOP, répondre à ce besoin de nomadisme conduit à des gains de productivité de l'ordre de 20%. Le nomadisme nécessite la mise en œuvre de politiques de sécurité interne et de gestion de la mobilité.

- l'authentification : toute personne ou tout équipement se connectant sur le réseau doit préalablement être authentifié. Les employés sont en général répertoriés dans un annuaire. Pour les visiteurs, il faut mettre en place une gestion de leur compte d'accès : création, suppression, droits.
- un accès Internet simple et automatique pour tous les visiteurs sans surcharge de travail pour le personnel d'accueil et sans besoin d'assistance technique.
- la réponse aux obligations légales : l'obligation en vigueur en France et en Europe pour l'entreprise de conserver les données de connexion pendant une durée 12 mois (décret du 24 mars 2006) de 6 à 24 mois en Europe (directive 2006/24/CE),
- la sécurisation des informations circulant sur le réseau et le cloisonnement des flux.

➤ La solution UCOPIA

UCOPIA répond à l'ensemble des besoins de sécurisation et de mobilité des entreprises.

Toutes les fonctions sont intégrées dans deux gammes d'appliance : UCOPIA Express et UCOPIA Advance. Les 2 gammes permettent de proposer très simplement un accès réseau aux visiteurs et aux employés, tout en se conformant aux obligations de sécurité et légales et sans mobiliser un personnel spécialisé pour opérer ce service. UCOPIA Express répond précisément à des besoins de type PME ou hotspots publics et privés. UCOPIA Advance offre des fonctions complémentaires à Express pour mieux répondre aux besoins des moyennes et grandes organisations (équilibre de charge, intégration fine avec les infrastructures réseau / solutions de sécurité en place, architecture multi-sites).

La réponse UCOPIA aux exigences légales de sécurité et de traçabilité

(Décret du 24 mars 2006 en France, 2006/24/CE en Europe)
Grâce aux mécanismes d'authentification, de contrôle et de filtrage des flux et de journalisation dans une base de données SQL, UCOPIA garantit la sécurité des utilisateurs, du réseau et la traçabilité des connexions. UCOPIA stocke dans un journal l'historique des connexions (qui a fait quoi et quand), mécanisme indispensable pour faire face aux exigences légales de la loi contre le terrorisme.

L'accueil du visiteur : confort et simplicité

Grâce aux outils de création de comptes utilisateur UCOPIA, et à l'authentification des utilisateurs par portail Web, l'accueil du visiteur est simple et sans contraintes.

UCOPIA permet en toute simplicité de :

- fournir un mot de passe (administration déléguée, création de comptes en masse lors de séminaire),
- définir les droits (Internet, messagerie, imprimante, bande passante),
- déterminer les modalités de connexion (par exemple de 10h à 12h dans la salle de réunion, forfait par jour, crédit de 3 heures pour une semaine, ...),
- fournir un coupon contenant les informations nécessaires à la connexion, .
- laisser le visiteur se déclarer tout seul sur Internet et lui envoyer immédiatement un mot de passe par SMS sur son téléphone mobile, .
- résilier automatiquement les droits du visiteur à son départ. Tout ceci peut être accompli par un personnel n'ayant pas de compétences techniques (hôtesse d'accueil, organisateur de réunion...), par mail ou par boîte vocale.

L'accès zéro configuration, zéro assistance technique pour les visiteurs

Grâce à UCOPIA, les visiteurs peuvent se connecter avec leur propre PC, et bénéficient du confort d'un accès zéro configuration. L'usage est simple pour le visiteur et ne nécessite pas d'assistance technique.



Sécurité adaptée aux entreprises

UCOPIA permet de définir des niveaux de sécurité adaptés aux différentes populations des entreprises : employés, prestataires, collaborateurs, clients... Pour chacune de ces populations, le mode d'authentification peut être personnalisé ainsi que les droits d'accès aux applications/ressources du réseau. UCOPIA s'adapte aux architectures VLAN mises en place sur le réseau filaire.

Contrôle d'accès

Contrôle d'accès par profil dépendant du contexte : les employés et visiteurs n'ont bien sûr pas les mêmes droits. De plus, les applications auxquelles une personne aura accès dépend de son profil : visiteur (collaborateur, client, prestataire, ...) ou employé et du contexte : heure, lieu.

Renforcement de la sécurité sur le réseau filaire

UCOPIA peut également gérer les connexions filaires (Ethernet, DSLAM, CPL), pour les postes en libre-service par exemple : authentification, contrôle d'accès, nomadisme. L'environnement de connexion filaire ou sans fil devient ainsi plus sûr et confortable pour les utilisateurs.

Témoignage de RIP CURL EUROPE SAS

Afin de permettre à ses salariés, ses visiteurs ou ses sous-traitants d'accéder au réseau par le Wi-Fi, RIP CURL EUROPE SAS, un des leaders mondiaux du monde du surf, a choisi UCOPIA Communications pour faciliter l'accès au réseau de l'entreprise ou au réseau Internet par le Wi-Fi. « Nous avons, entre autres, des préoccupations financières, et seul UCOPIA pouvait s'adapter au matériel déjà mis en place, alors qu'avec les autres solutions, nous aurions été obligés de modifier tout ou partie de notre installation, et donc de supporter de nouvelles dépenses »,

souligne Jean-Pierre Bordenave, Manager Systems & Architecture de Rip Curl. « Dans le même temps, nous avons constaté la simplicité d'utilisation de la solution d'UCOPIA : un portail captif de délégation utilisé par l'accueil peut fournir un accès à un Internet ou tout autre service (SMTP, FTP, telnet,...) suivant des profils définis à tout nouveau visiteur en toute sécurité pour le réseau de l'entreprise. »

Jean-Pierre BORDENAVE, Manager Systems & Architecture de RIP CURL EUROPE SAS.