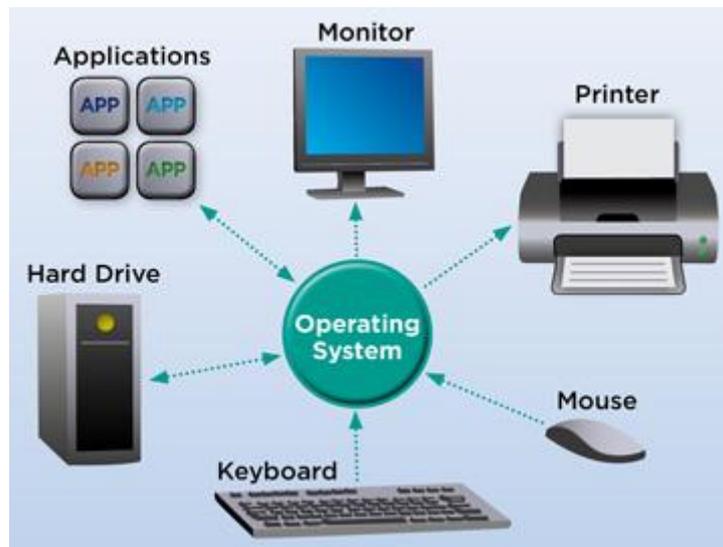


Service Managed Secured Workplace – SV07

Description

Le service permet une gestion centralisée des éléments suivants :

1. Microsoft Windows (plus récent)
2. Microsoft Office O365 (plus récent)
3. Apple Mac OSX
4. Système d'exploitation Android
5. Gestion centralisée des imprimantes réseau.
6. Gestion des logiciels clients
7. Gestion des correctifs de sécurité



Gestion des périphériques (SV07.01)

Description

Le service fournit une solution de gestion centralisée pour les mises à jour des postes de travail (smartphone, tablette, ordinateur portable) connectés au réseau de l'entreprise.

Caractéristiques

Le service de gestion des postes clients permet de gérer de manière centralisée les mises à jour des périphériques suivants :

- Systèmes Microsoft Windows
- Apple Mac OSX
- Android Os

Le service de gestion des postes clients permet de gérer les mises à jour de presque toutes les applications Microsoft.

La prise en charge à distance des appareils est possible quel que soit leur système d'exploitation et leur emplacement.

- Une connexion Internet est requise

Conditions

1. Il est nécessaire de disposer d'un serveur M365-E3 par utilisateur
1. Connexion réseau de 1 Go minimum à la Chancellerie.
2. Abonnez-vous au service de gestion des droits d'accès

CONTACT : 02 / 501 04 11 - ICT.kanselarij@premier.fed.be



* ICT Chancellerie utilise Intune et SCCM pour gérer le service.

Sauvegarde des données

Centralisation et fourniture de journaux de bord.

Protection des données

Tous les membres du personnel présents qui ont accès à l'infrastructure disposent d'une habilitation de sécurité du type « secret » pour le niveau national.

Service & SLA :

- L'exploitation et la maintenance du service central sont assurées 24 heures sur 24.
 - Alarmes et rapportage.
- Critique 24-7 (cfr. la description du contrat SLA dans le fichier Service 1. Support).

File Services (SV07.02)

Description

Permet d'accéder à un dossier du serveur NAS de l'entreprise.

Ce service fournit un espace de stockage sécurisé pour les stations de travail partenaires.

Ce service fournit un accès Internet sécurisé aux stations de travail des clients (smartphone, tablette, station de travail, ordinateur portable) connectées au réseau de l'entreprise.

Caractéristiques

Le service permet la gestion centralisée :

- Du filtrage des données à l'aide d'un antivirus
- Du stockage de données confidentielles et sensibles
- De la gestion des accès en cas de stockage partagé
- Du contrôle de l'accès à ces espaces de stockage.

Conditions :

- Il est nécessaire de disposer d'un compte dans AD
- Être connecté au réseau de la chancellerie.

Service et SLA :

1. Connexion Internet 24 h/24 et 7 j/7 disponible avec dispositif antivirus et filtrage des URL et du contenu. Le filtrage peut être adapté à vos besoins professionnels.
2. Critique 24-7 (cfr. la description du contrat SLA dans le fichier Service 1. Support).

Sauvegarde des données

Fourniture de journaux de bord.

Protection des données

Tous les membres du personnel présents qui ont accès à l'infrastructure disposent d'une habilitation de sécurité du type « secret » pour le niveau national.

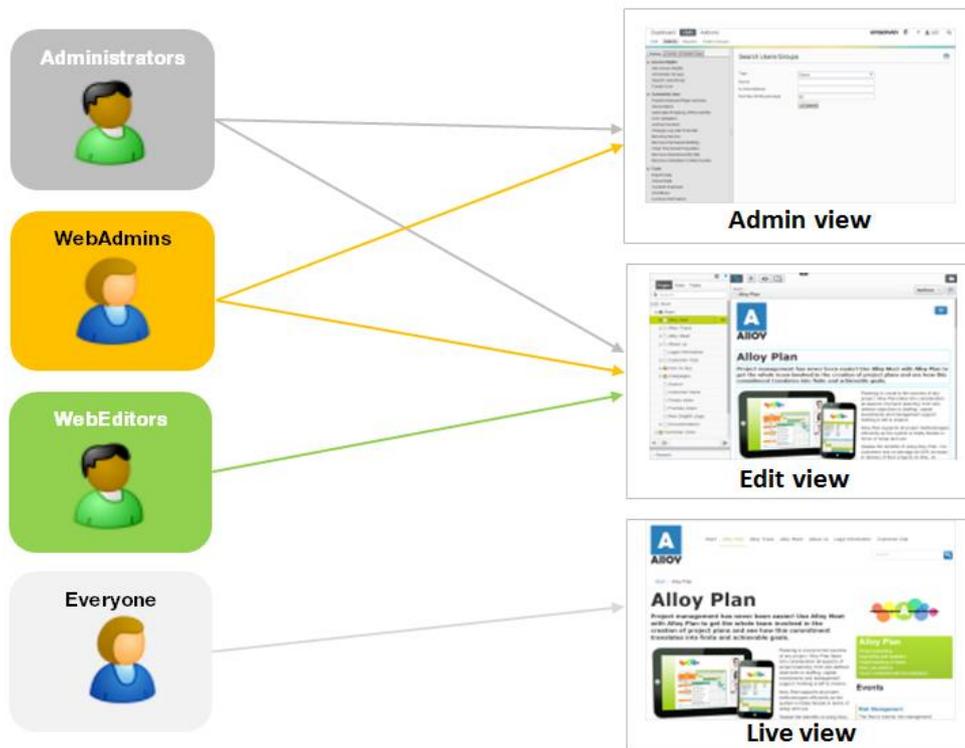
Droits d'accès (SV07.03)

Description

Gestion centralisée de l'identification et de l'autorisation d'une entité emprunteuse dans le cadre de l'utilisation du catalogue de services d'ICT Chancellerie.

Caractéristiques

Les droits d'accès sont les autorisations dont dispose un utilisateur ou une application informatique pour lire, écrire, modifier, supprimer ou accéder d'une autre manière à une ressource numérique ; pour modifier des configurations ou des paramètres, ou pour ajouter ou supprimer des applications.



Conditions

1. Il est nécessaire de disposer d'un serveur M365-E3 par utilisateur.

Service et SLA :

2. L'exploitation et la maintenance du service central sont assurées 24 heures sur 24.
CONTACT : 02 / 501 04 11 - ICT.kanselarij@premier.fed.be

3. Alarmes et rapportage :

1. Critique 24-7 (cf. La description SLA dans la fiche de support).

Sauvegarde des données

Centralisation et fourniture de journaux de bord.

Protection des données

Tous les membres du personnel présents qui ont accès à l'infrastructure disposent d'une habilitation de sécurité du type « secret » pour le niveau national.

Service d'impression (SV07.04)

Description

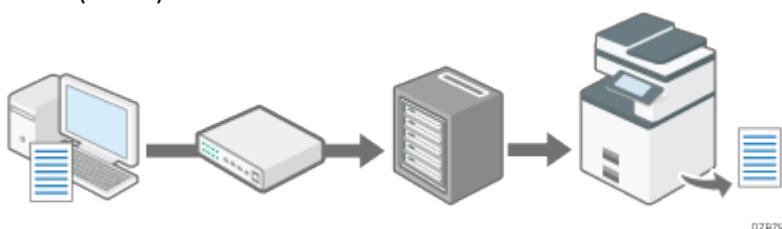
Il s'agit d'une gestion centralisée des imprimantes réseau.

Managed Print Services permet de gérer votre parc d'imprimantes pour une meilleure visibilité.

Lorsque vous vous connectez à une imprimante sur un serveur d'impression, le client de connexion recherche les pilotes appropriés sur le serveur d'impression. Une fois les pilotes installés sur le serveur, ils sont automatiquement téléchargés et configurés pour le client. Toutefois, si les pilotes ne sont pas présents, vous êtes invité à les sélectionner et à les installer.

Caractéristiques

- La configuration est effectuée avec le serveur FollowMe Simplifie et automatise l'impression.
- Impression centralisée ou directe.
- Print Anywhere (Cloud)



Conditions

- Connexion réseau d'au moins 1 Go à la Chancellerie
- Propriétaire de vos imprimantes réseau.
- Posséder vos propres cartouches de papier et d'encre
- Avoir un contrat de maintenance pour vos imprimantes
- Abonnez-vous au service de gestion des droits d'accès

Service et SLA :

- L'exploitation et la maintenance du service central sont assurées 24 heures sur 24.
- Alarmes et rapportage.

CONTACT : 02 / 501 04 11 - ICT.kanselarij@premier.fed.be



- Critique 24-7 (cf. La description SLA dans la fiche de support).

Sauvegarde des données

- Centralisation et disponibilité des journaux
- Scanning des statistiques

Protection des données

Tous les membres du personnel présents qui ont accès à l'infrastructure disposent d'une habilitation de sécurité du type « secret » pour le niveau national.

Workplace VPN (SV07.05)

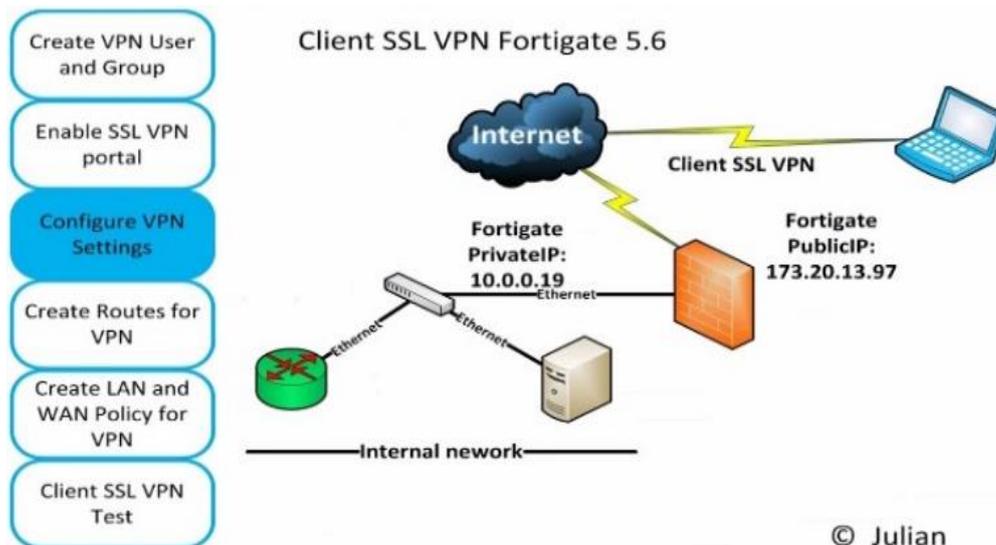
Description

Les VPN offrent la possibilité d'établir une connexion réseau sécurisée en utilisant les services sécurisés de la Chancellerie. Les VPN cryptent votre trafic Internet et masquent votre identité en ligne. Il est donc plus difficile pour un tiers de suivre vos activités en ligne et de voler vos données.

Caractéristiques

- Fortinet EMS Client (dernière version stable et testée).
- Reconnexion automatique* (toujours activée)
- Prise en charge des ordinateurs portables et de bureau
- L'agent Zero Trust, disponible uniquement sur FortiClient PRO, prend en charge
 - ZTNA-tunnels,
 - connexion unique (SSO),
 - Contrôle du statut du périphérique
- Client VPN
- Web Filter
- Vulnerability scan
- Device posture check.

Cette solution VPN n'est pas disponible si votre ordinateur est connecté au réseau interne ICT Shared Services. Du moins, si vous travaillez sur votre ordinateur dans les locaux de votre organisation.



Conditions

- Abonnez-vous au service de gestion des droits d'accès
- FortiVPN Pro est obligatoire sur les appareils non gérés par la Chancellerie.

Service et SLA :

- L'exploitation et la maintenance du service central sont assurées 24 heures sur 24.
- Alarmes et rapportage.
- Critique 24-7 (cfr. La description SLA dans la fiche de support).

Sauvegarde des données

Centralisation et fourniture de journaux de bord.

Protection des données

Tous les membres du personnel présents qui ont accès à l'infrastructure disposent d'une habilitation de sécurité du type « secret » pour le niveau national.

*Uniquement disponible sur FortiClient Pro