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

Gestionnaire de 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.

Fonctionnalités

Le service Gestion des postes clients permet une gestion centralisée des mises à jour pour les appareils suivants :

- Microsoft Windows Systems
- Apple Mac OSX
- Android Os

Le service Gestion des postes clients permet de gérer les mises à jour de presque toutes les applications non Microsoft.
Le support à distance des appareils est possible, quel que soit le système d'exploitation et l'emplacement.

- Une connexion Internet est requise

Conditions

1. Il est nécessaire d'avoir 1 M365-E3 par utilisateur
1. Connexion réseau d'au moins 1 Go avec la Chancellerie.

2. Abonnez-vous au service de gestion des droits d'accès

* La Chancellerie TIC utilise Intune et SCCM pour gérer le service.

Sauvegarde des données

Centralisation et livraison des journaux.

Sécurité des données

Tout le personnel présent ayant accès à l'infrastructure dispose d'une habilitation de sécurité de type « secret » pour le niveau national.

Service & SLA :

- L'exploitation et la maintenance du service central sont assurées 24 heures sur 24.
    - Alerte et signalement.
- Critical 24h/24 (cf. la description SLA dans le fichier Service 1. Soutien).

Services de fichiers (SV07.02)

Description

Permet d'accéder à un dossier sur le serveur NAS de l'entreprise. Le service

offre un espace de stockage sécurisé pour les postes de travail des

partenaires.

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

Fonctionnalités

Le service permet la gestion centralisée de :

- Filtrage des données par un programme antivirus
- Espace de stockage pour les données confidentielles et sensibles
- Contrôle d'accès dans le cas d'espaces de stockage partagés
- Contrôlez l'accès à ces espaces de stockage.

Conditions :

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

Service et SLA :

1. Connexion Internet disponible 24h/24 et 7j/7 avec filtrage d'URL et de contenu et un dispositif antivirus. Le filtrage peut être personnalisé pour répondre aux besoins de votre entreprise.

2. Critical 24h/24 (cf. la description SLA dans le fichier Service 1. Soutien)

Sauvegarde des données

Fourniture de journaux.

Sécurité des données

Tout le personnel présent ayant accès à l'infrastructure dispose d'une habilitation de sécurité de type « secret » pour le niveau national.

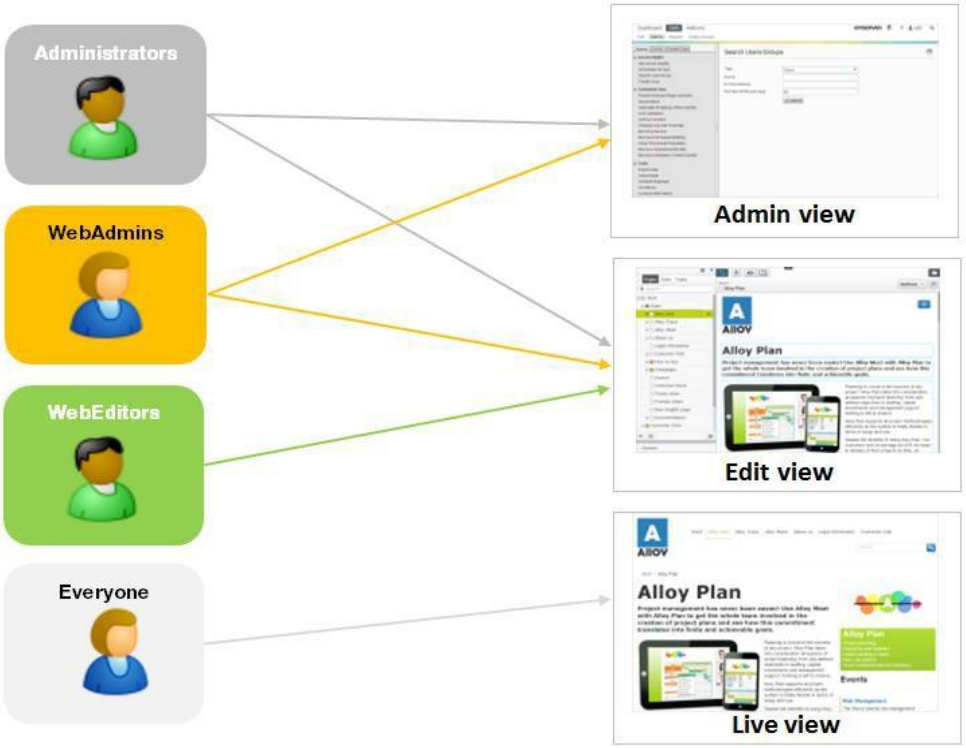
Droits d'accès (SV07.03)

Description

Gestion centralisée de l'identification et de l'autorisation d'une entité utilisateur dans le contexte de l'utilisation du Catalogue des services de la Chancellerie TIC.

Fonctionnalités

Les droits d'accès sont les autorisations qu'un utilisateur ou une application informatique individuelle dispose pour lire, écrire, modifier, supprimer ou autrement accéder à une ressource numérique ; Changez les configurations ou les réglages, ou ajoutez ou supprimez des applications.



Conditions

1. Il est nécessaire d'avoir 1 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. Alerte et signalement.

1. Critique 24h/24 (cf. la description SLA dans la fiche de soutien).

Sauvegarde des données

Centralisation et livraison des journaux.

Sécurité des données

Tout le personnel présent ayant accès à l'infrastructure dispose d'une habilitation de sécurité de type « secret » pour le niveau national.

Service d'impression (SV07.04)

Description

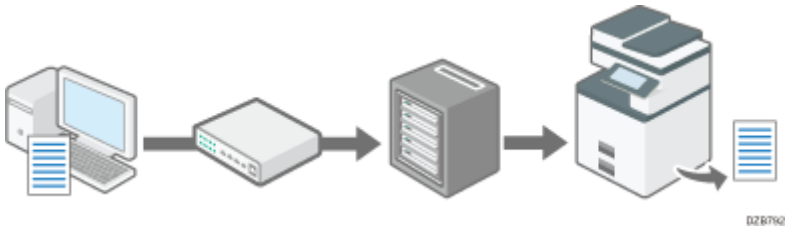
Il s'agit d'une gestion centralisée des imprimantes réseau.

Les services d'impression gérés vous permettent de gérer votre flotte d'imprimantes pour une meilleure visibilité.

Lorsque vous vous connectez à une imprimante sur un serveur d'impression, le client de connexion vérifie le serveur d'impression pour les bons pilotes. Si les pilotes sont installés sur le serveur, ils sont automatiquement téléchargés et configurés pour le client. Cependant, si les pilotes ne sont pas présents, il vous sera demandé de les sélectionner et de les installer.

Fonctionnalités

- La configuration se fait avec le serveur FollowMe, ce qui simplifie et automatise l'impression.
- Impression centralisée ou directe à l'imprimante.
- Imprimer n'importe où (Cloudprint)



Conditions

- Connexion réseau d'au moins 1 Gb à la Chancellerie
- Propriétaire de vos imprimantes réseau.
- Possédez votre propre papier d'impression et cartouches d'encre
- Obtenez 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.

- Alerte et signalement.
- Critique 24h/24 (cf. la description SLA dans la fiche de soutien).

Sauvegarde des données

- Centralisation et disponibilité des journaux
- Statistiques de balayage

Sécurité des données

Tout le personnel présent ayant accès à l'infrastructure dispose d'une habilitation de sécurité de type « secret » pour le niveau national.

VPN au travail (SV07.05)

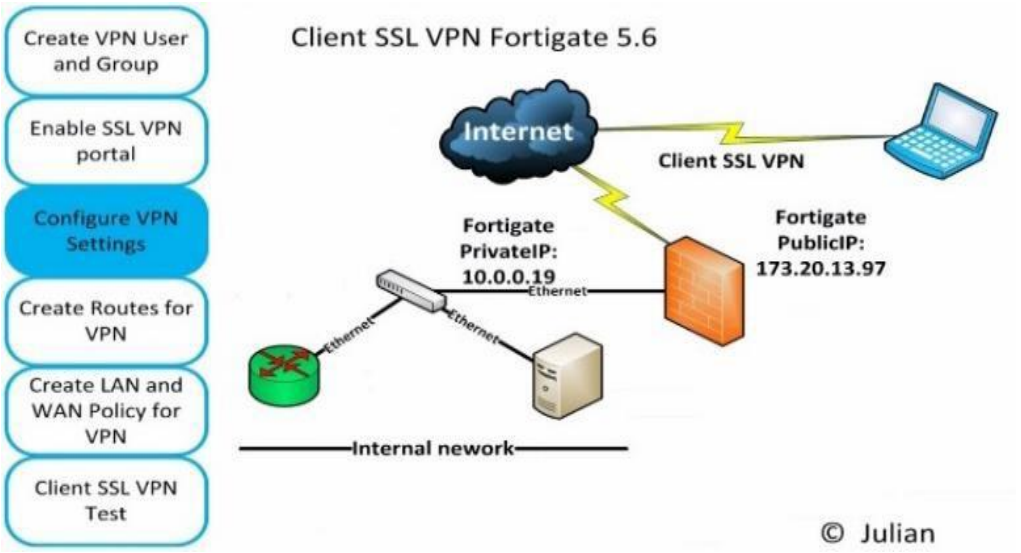
Description

Le VPN offre la possibilité d'établir une connexion réseau sécurisée lors de l'utilisation des services sécurisés de la Chancellerie. Les VPN chiffrent votre trafic internet et masquent votre identité en ligne. Cela rend plus difficile pour des tiers de suivre votre activité en ligne et de voler des données.

Fonctionnalités

- Client EMS Fortinet (dernière version stable et testée).
- Reconnexion automatique* (fonction Toujours activée)
- Pris en charge sur ordinateur de bureau et portable
- L'agent Zero Trust, disponible uniquement sur FortiClient PRO, prend en charge
    - Tunnels ZTNA,
    - connexion unique (SSO),
    - Vérification de l'état de l'appareil
- VPN Client
- Filtre Web
- Balayage des vulnérabilités
- Vérification de la posture de l'appareil.

Cette solution VPN n'est pas disponible si votre ordinateur est connecté au réseau interne des services ICT Shared Services. C'est-à-dire, si vous travaillez sur votre ordinateur dans les bâtiments 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.
- Alerte et signalement.
- Critique 24h/24 (cf. la description SLA dans la fiche de soutien).

Sauvegarde des données

Centralisation et livraison des journaux.

Sécurité des données

Tout le personnel présent ayant accès à l'infrastructure dispose d'une habilitation de sécurité de type « secret » pour le niveau national.

*Disponible uniquement sur FortiClient Pro