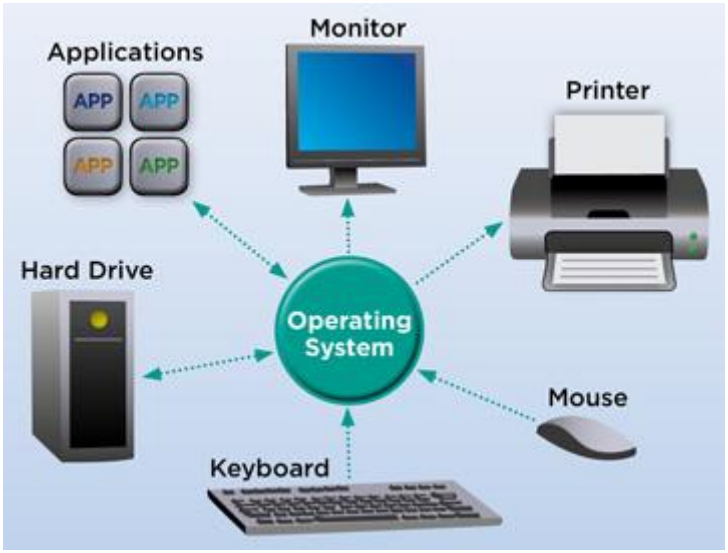
Secured Managed Workplace Service – SV07

Description

The service allows for centralised management of the following:

- Microsoft Windows (latest)
- Microsoft Office O365 (latest)
- Apple Mac OSX
- Android OS
- Network printers
- Client software
- Security patches



Device Management (SV07.01)

Description

The service offers a centralised solution for managing updates to devices (smartphones, tablets, laptops) connected to the corporate network.

Features

The Device Management service allows for centralised management of updates to:

- Microsoft Windows (latest)
- Microsoft Office O365 (latest)
- Apple Mac OSX
- Android OS

Preconditions

- Have one M365 E3 per user
- Have a network connection with the Chancellery (minimum 1 Gb)
- Have your own network printers
- Subscribe to the Access Right Management service

Data backup
Centralisation and provision of logs

Data security
All members of staff involved who have access to the infrastructure hold national 'secret' level security clearance.

File Services (SV07.02)

Description
This service allows access to a corporate server folder.

The service provides a secure storage space for client devices.

The service provides secure internet access for client devices (smartphones, tablets, workstations, laptops) connected to the corporate network.

Features
The service allows for centralised management of:

- Data filtering by anti-virus software
- Storage space for confidential and sensitive data
- Access management for shared storage spaces
- Auditing of access to these storage spaces

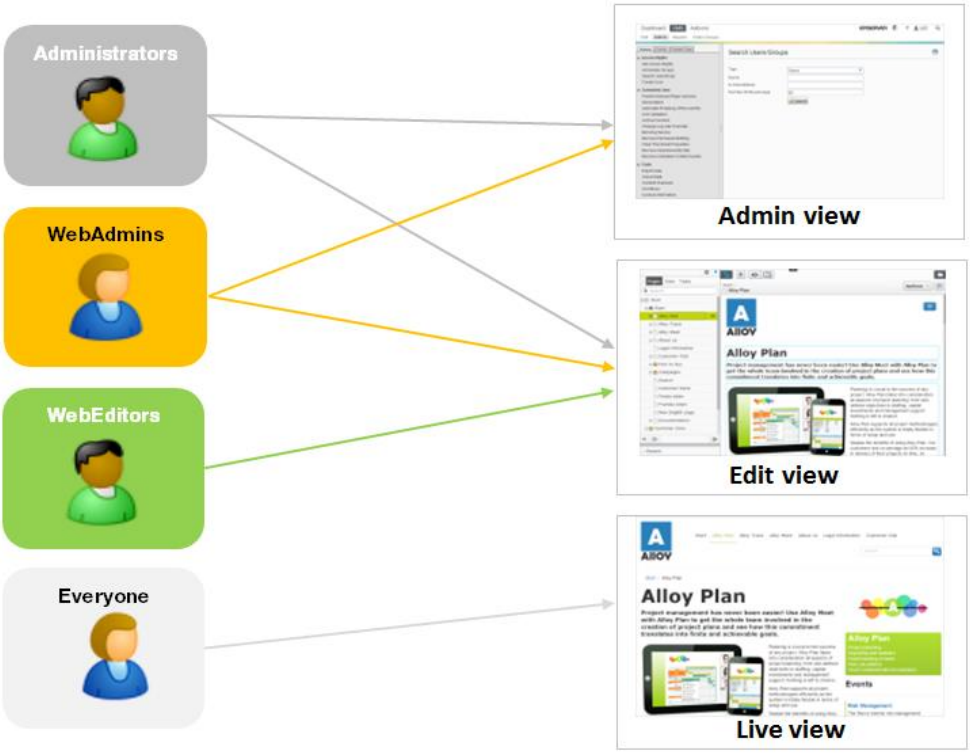
Data backup
Provision of logs

Data security
All members of staff involved who have access to the infrastructure hold national 'secret' level security clearance.

Access Rights (SV07.03)

Description
This service offers centralised management of user-entity identification and authorisation in connection with use of the ICT Chancellery service catalogue.

Features
Access rights are the permissions an individual user or a computer application holds to read, write, modify, delete or otherwise access a digital resource, to change configurations or settings, or add or remove applications.



Preconditions

- Have one M365 E3 per user

Data backup

Centralisation and provision of logs

Data security

All members of staff involved who have access to the infrastructure hold national 'secret' level security clearance.

Print Service (SV07.04)

Description

This service involves centralised management of network printers.

With managed print services, it allows your print fleet to be managed for enhanced visibility.

When you connect to a printer on a print server, the connecting client looks for the appropriate drivers on the print server. If the drivers are installed on the server, the drivers are automatically downloaded and configured for the client. However, if the drivers are not present, you are prompted to select and install the drivers.

Features

- Configuration based on FollowMe server, which simplifies and automates printing
- Centralised printing or direct to printer

CONTACT: +32 (0)2 501 04 11 – ICT.chancellerie@premier.fed.be

Preconditions

- Have your own network printers
- Have your own printing paper and ink cartridges
- Have a maintenance contract for your printers
- Subscribe to the Access Right Management service

Data backup

- Centralisation and provision of logs
- Scan statistics

Data security

All members of staff involved who have access to the infrastructure hold national 'secret' level security clearance.

Workplace VPN (SV07.05)

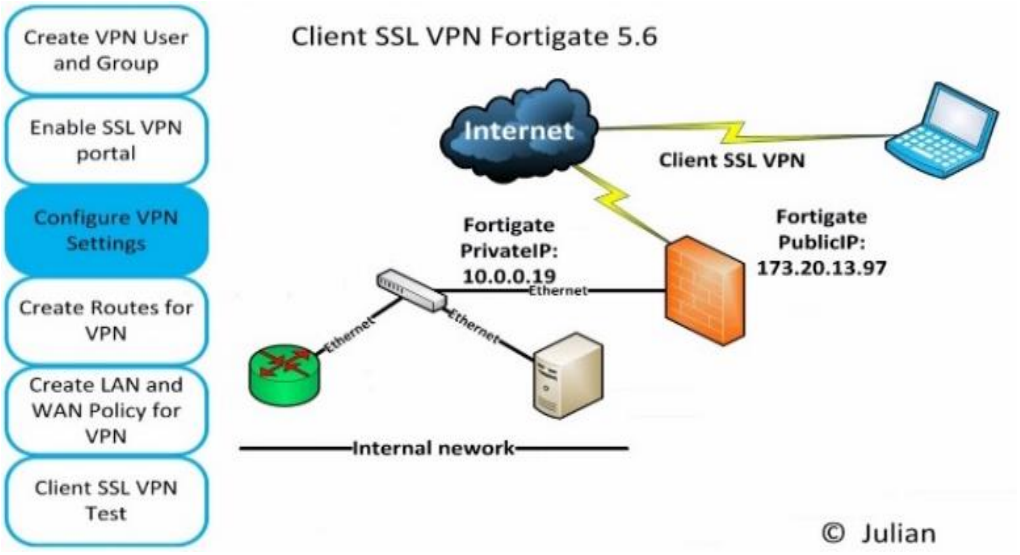
Description

The VPN lets you create a secure network connection when using secure Chancellery services. VPNs encrypt your internet traffic and conceal your identity online, making it harder for third parties to track your online activities and steal data.

Features

- Fortinet VPN (latest stable and tested version)
- Auto reconnect* ('Always On')
- Supported on desktop and laptop
- The Zero Trust Agent, only available on FortiClient Pro, supports
    - ZTNA tunnels,
    - single sign-on (SSO),
    - device posture check.

This VPN solution is not available if your computer is connected to the ICT Shared Services internal network, i.e. if you are working on your computer in your organisation's buildings.



Preconditions

- Subscribe to the Access Right Management service
- FortiVPN Pro mandatory on devices not managed by the Chancellery

Data backup

Centralisation and provision of logs

Data security

All members of staff involved who have access to the infrastructure hold national 'secret' level security clearance.

CONTACT: +32 (0)2 501 04 11 – ICT.chancellerie@premier.fed.be