Org@Work

Functional & Technical presentation

LUNDANO

Index
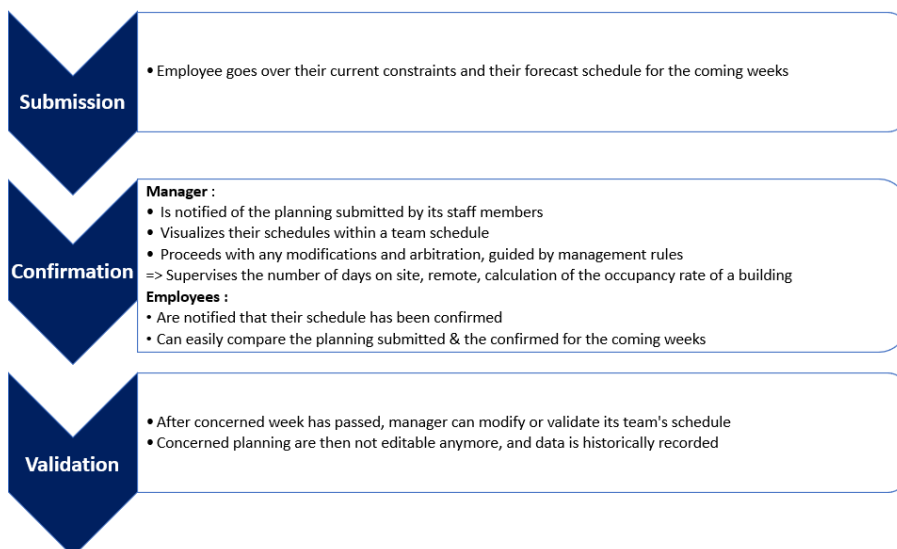
I. Presentation

Description

Org@Work is a solution dedicated to the management of work organization and enables employees to report their constraints and scheduling wishes, over a configurable forecast period. Information is shared in real time by the manager, who thus has an aggregated view of the provisional schedules of its team. On this basis, and by integrating the framework set by the organization (remote agreement, premises access gauge, etc.), managers can then modify or confirm the schedules.
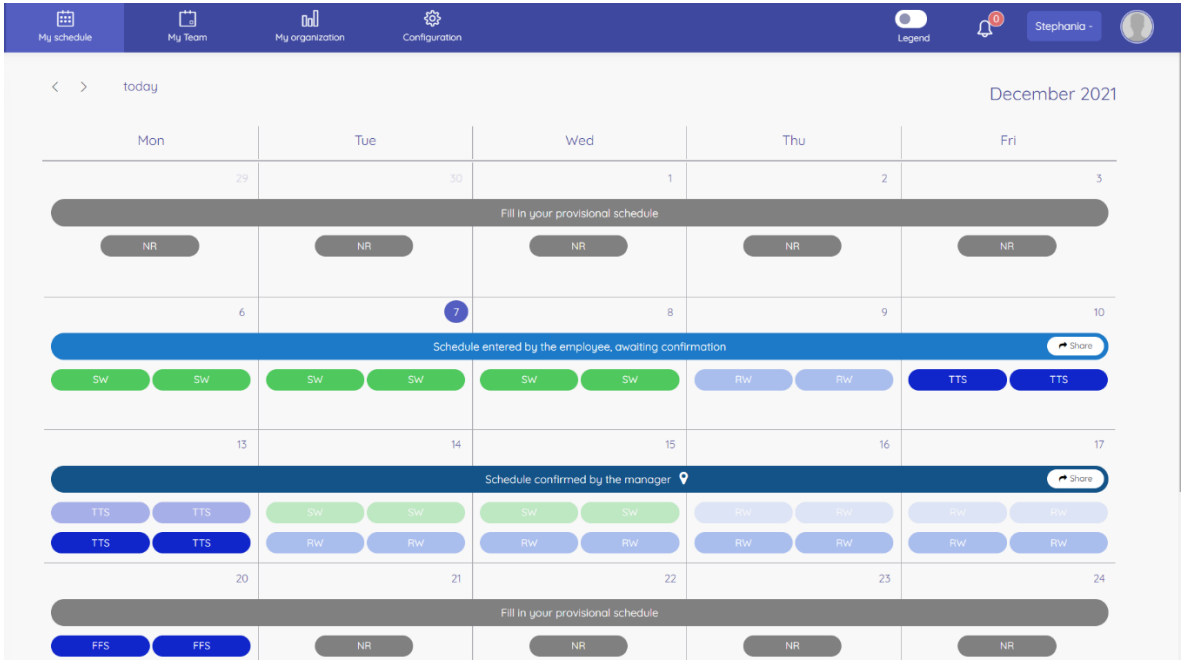
Global overview

Employee

- I suggest a schedule taking my aspirations and constraints into account, within the framework defined by the organization
- I come back to my workplace in good conditions, guided by clear rules
- My health and safety are taken into account by my organization
- I have all elements to organize on site exchanges

Org@Work

- ☑ **Manage on site vs remote working planning**
- ☑ **Ease decision taking within the framework set by my organisation & employees' needs**
- ☑ **Workspace management : monitor occupation rate, be able to locate immediately teams in the case of close contact (Covid 19)**
- ☑ **Collaborative tool**
- ☑ **Reportings & dashboards**

Direct Manager

- Based on the proposals of my team, I manage the balance between on site & remote working within the framework set by the organization
- I organize the collective times of the team
- I can manage specific or risky situations in real time
- I manage the occupancy rate of the workplace of my team

Top Management

- I define the framework of the work organization & provide the workforce with the appropriate tools
- I have reliable management data to adapt and reorient decisions in real time, according to the evolution of the situation
- I optimize workspaces management

Workforce

- We share clear & common rules, taking into account each employee constraints
- We have up-to-date information to facilitate exchanges of information
- We foster a sense of belonging to a responsible collective

Workflow

Submission
- Employee goes over their current constraints and their forecast schedule for the coming weeks

Confirmation

Manager :
- Is notified of the planning submitted by its staff members
- Visualizes their schedules within a team schedule
- Proceeds with any modifications and arbitration, guided by management rules
=> Supervises the number of days on site, remote, calculation of the occupancy rate of a building

Employees :
- Are notified that their schedule has been confirmed
- Can easily compare the planning submitted & the confirmed for the coming weeks

Validation
- After concerned week has passed, manager can modify or validate its team's schedule
- Concerned planning are then not editable anymore, and data is historically recorded

Detailed functionalities

| Category	Functionalities
Management parameters / rules	- Management of the number of days (min / max) on site, number of days (min / max) of remote; management of partial activity - Alert if any of the guidelines are not respected. - Allocation of the employee to a location (floor, wing, etc.) allowing easier management of the occupancy rate of a site, building or floor.
Workspace booking	- Workspace booking for employees regarding the privileges given by the organization to each employee - Possibility to evaluate the occupancy rate of each workspace as the employee confirm their planning
Planning management	- 3 planning stages: Submitted by the employee, confirmed by the manager, then "validated" - Once validated, the schedule is no longer editable and can be used as proof (% of presence on site in particular)
Planning views	- Planning accessible i) to employees within the same team, ii) to managers within the same department / function /… and iii) transversally to profiles of "super managers" to visualize all plannings (eg HR team)
Delegations & privileges	- Delegation: possibility to delegate rights in a personalized way - Privileges: management of access rights enabling visualizations at different levels of the organization
Reportings	- Pre-configured reports in the tool, in particular forecast analysis of remote rate or presence on site. Possibility of exporting full database for advanced analyzes and reports
HR repository	- Loading of the employees source file with basic information (office location, activity rate, etc.) and attachment to the planning manager.
GDPR	Org@Work is a GDPR compliant solution
Hosting	SaaS

Visualizations

Visualization by the employee of his planning and the planning manager's response
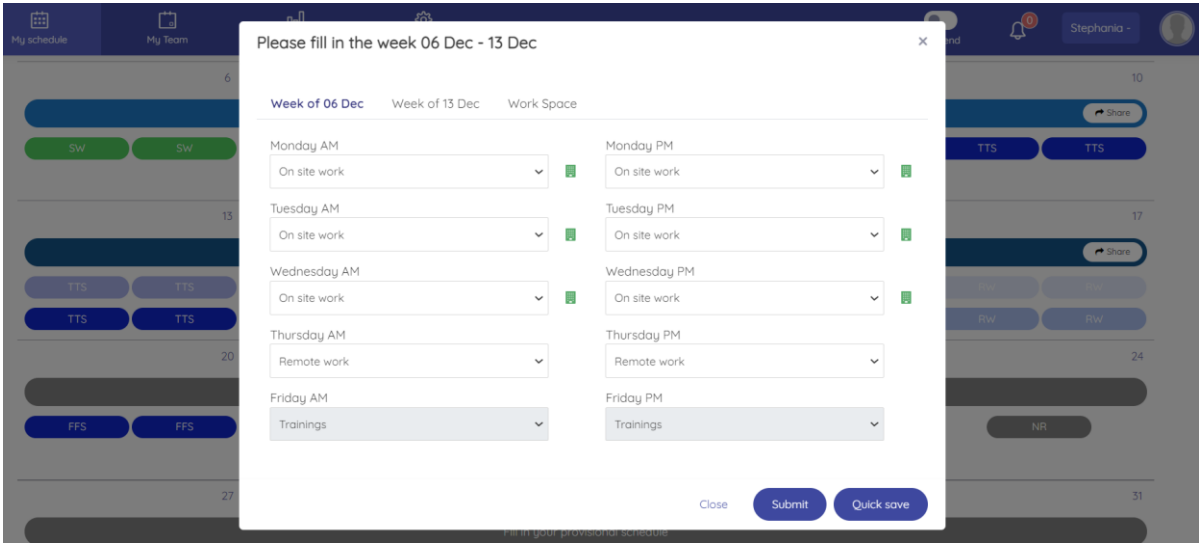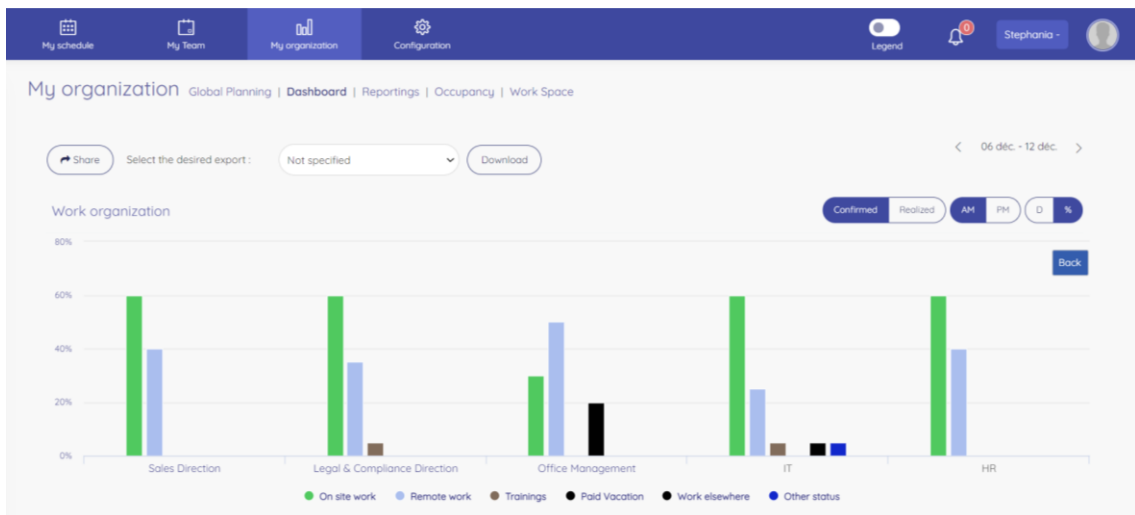

Filling of the provisional planning by the employee (1/2)
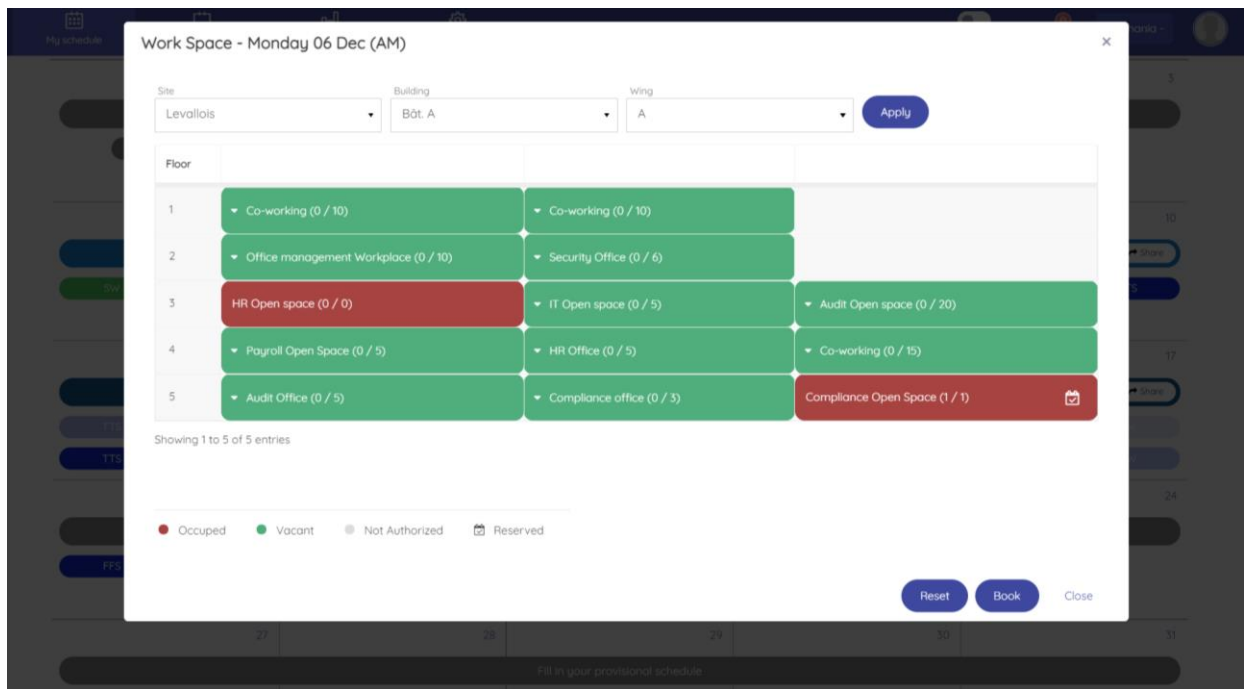
Filling of the provisional planning by the employee (2/2) – Openspace booking (optional)
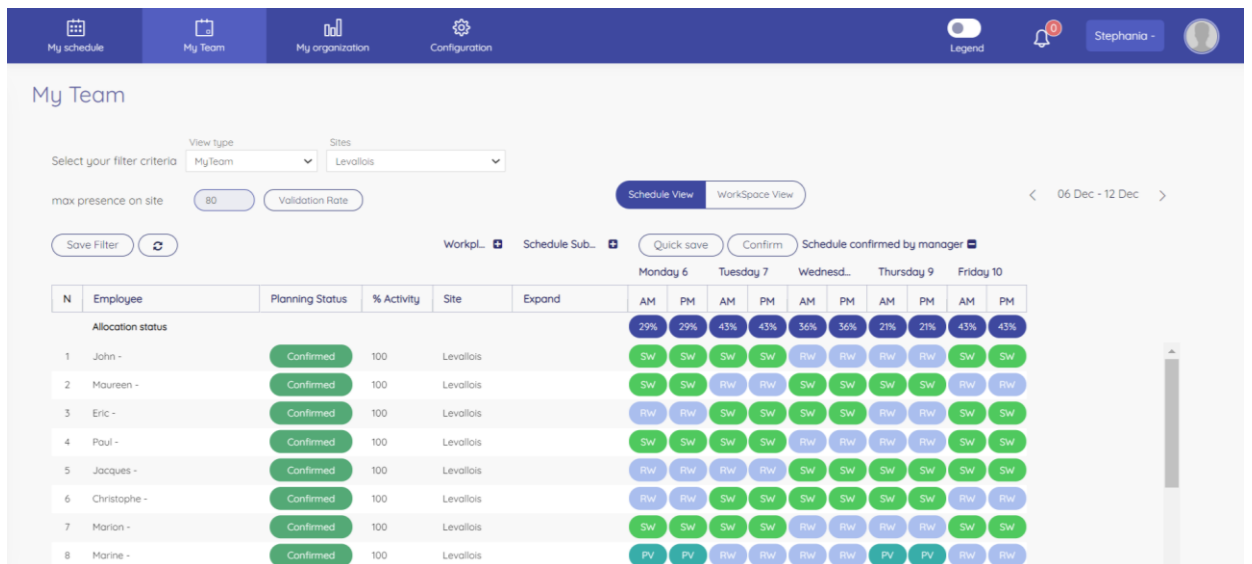
Visualization of a team's planning by the manager

Global vision of the company's work organization (depending of the user)

Visualization of the occupancy rate per team

Visualisation of the occupancy rate of all the company's buildings.

Detailed visualization of workspaces and indication of their availability

Org@Work and Outlook

Org@work is a solution integrated with Microsoft Outlook that allows:
- The visualization of on-site and remote participants in the meeting planning assistant
- The identification of the appropriate meeting room

Functional component:

The Org@Work add-in in Microsoft Outlook allows the Org@Work user to view the working status (on-site/remote) of the meeting participants directly from the Outlook scheduling assistant.

Scenario 1: the meeting participants are part of my Org@Work privilege

o **First use case: visualization of the working status of the participants at the meeting date and time**

The precision of the information available in the Add-in depends on the Org@Work privilege of the meeting organizer: if the meeting organizer can see the working status of the participants in Org@Work, then he will be able to see them in Outlook (they share the same department, direction, etc.)
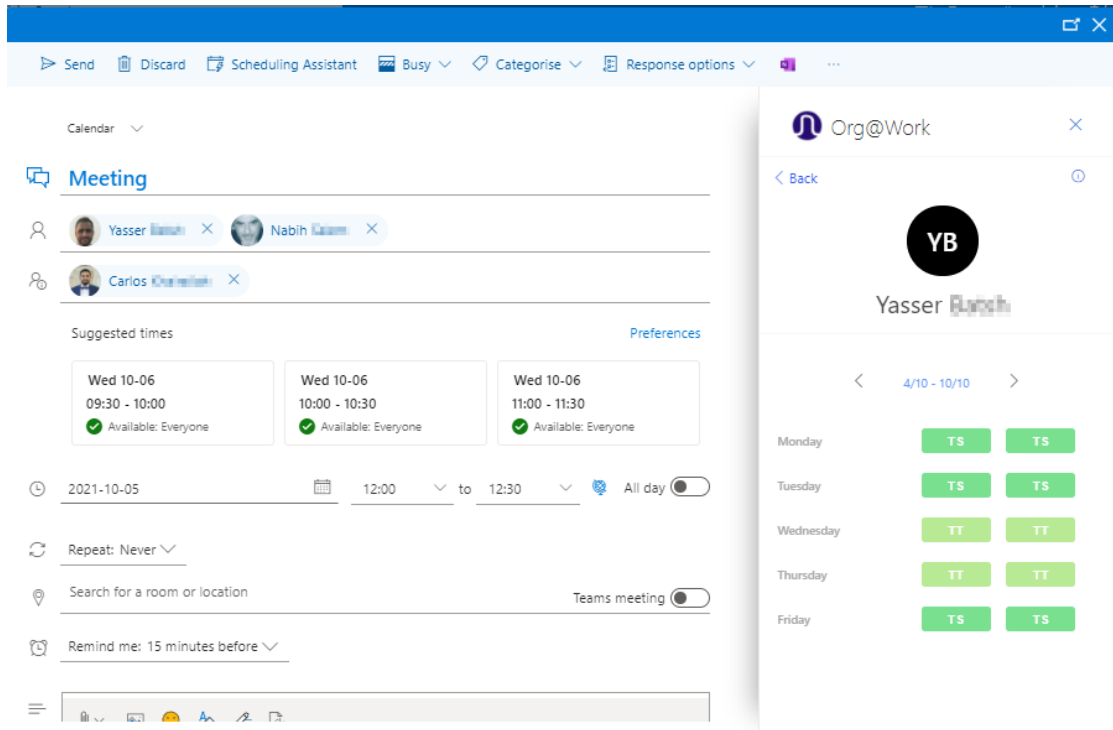
N.B.: the visible working status is the status Confirmed by the Planning Manager
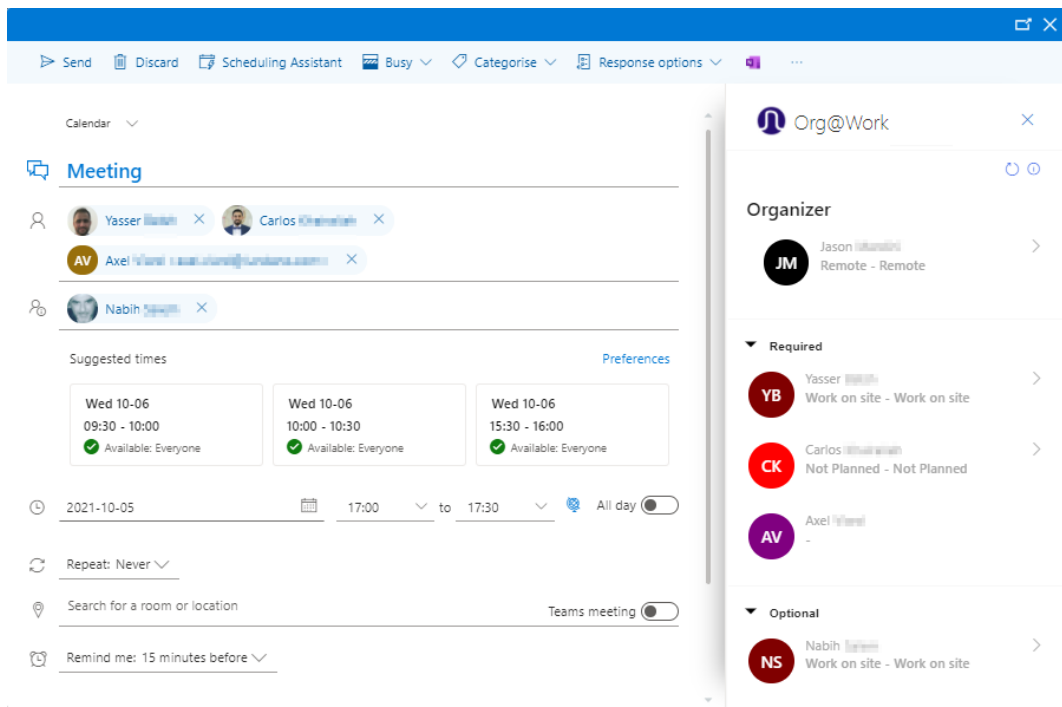
Visualization of the working status for the day of the meeting

- o **Second use case: visualization of the working status of the participants over the whole week**

By clicking on the name of one of the possible participants of the meeting, the organizer can visualize the planning of his colleagues and their working status over the whole week.


By clicking on the name of a potential participant, zoom and see his planning of the week

Scenario 2: the meeting participants are not part of my Org@Work privilege

- o **First use case: visualization of the working status of the participants at the date and time of the meeting**

In this case, the information available is reduced to "Busy" or "Available", without being able to see the reason for the absence (telework, business trip, leave, sick leave).

The Outlook add-in thus provides useful information while guaranteeing compliance with GDPR standards.
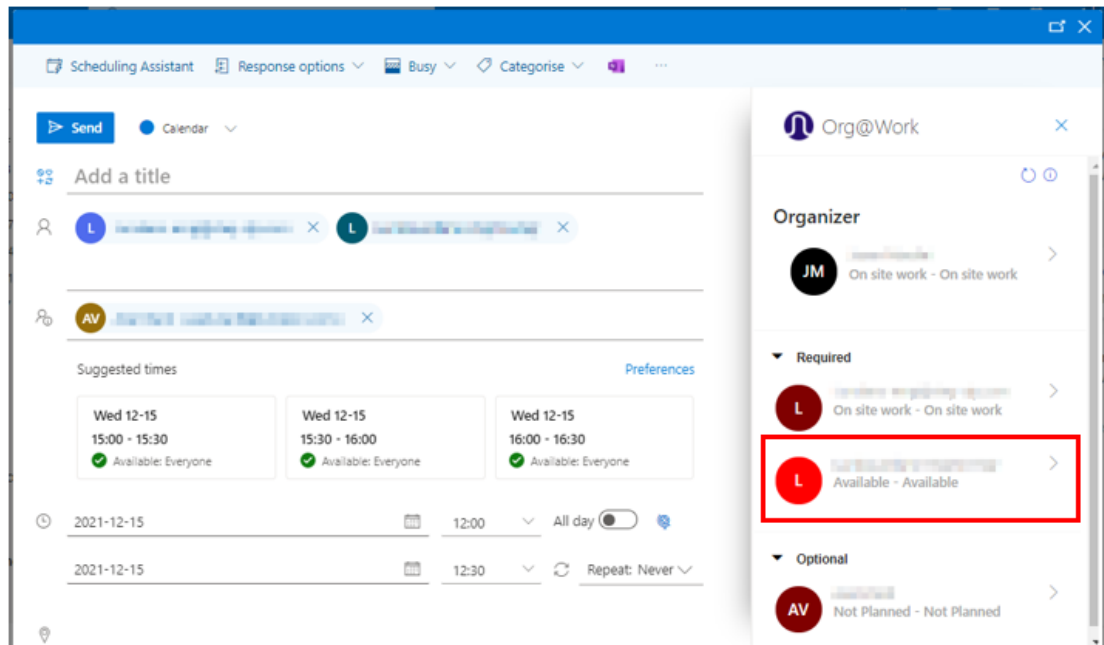
Viewing a generic working status for the day of the meeting

- o **Second use case: visualization of the working status of the participants over the whole week**

The information available for the entire week of the selected employee is also reduced to "Busy" or "Available".
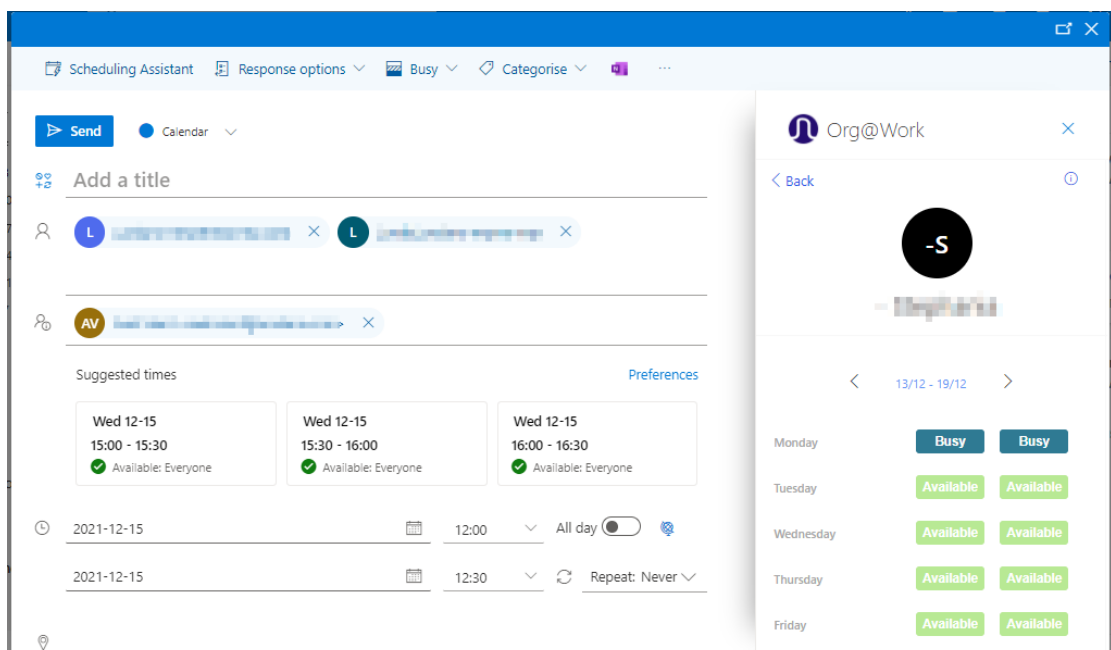
Visualisation of the working status for the whole week of a colleague by clicking on his name

<u>Technical component:</u>

For authentication when opening the Org@Work Add-in in Microsoft Outlook:
- o Method: WebToken to identify the user using Microsoft Office 365 authentication
- o Microsoft GraphAPI permissions:

Application Permission	Delegated Permission	Justification	Admin Consent Required?
	User.Read	Teams App SSO	No
	email	Teams App SSO	No
	offline_access	Teams App SSO	No
	OpenId	Teams App SSO	No
	profile	Teams App SSO	No

- o Data: User Open ID and User Profile (Name & Email/UPN) using Graph API

In the content of the Add-in:
- o Method: Org@Work Web API to retrieve work status information

Org@Work inside Teams

Integration of Org@Work in Teams meets the following objectives:

- Carry out Org@Work workflow in Teams to reducethe number of applications open for the user
- Facilitate access to key information (plannings, dashboards, etc.)
- Strengthen the collaborative component by sharing team information within Teams

Org@Work integrated into Teams enables:

- Direct access to the tool via a dedicated icon & simple navigation between Org@Work sections
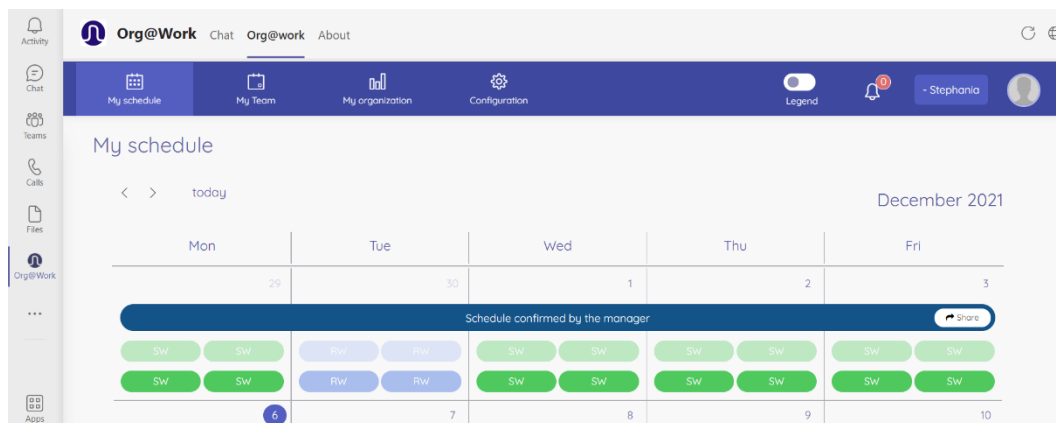
- Worfkflow is duplicated into Teams Bot, notifying managers of any entry/modification of a staff members' schedule. Manager can confirm temptative schedule fom the CTA button, or access team planning view.
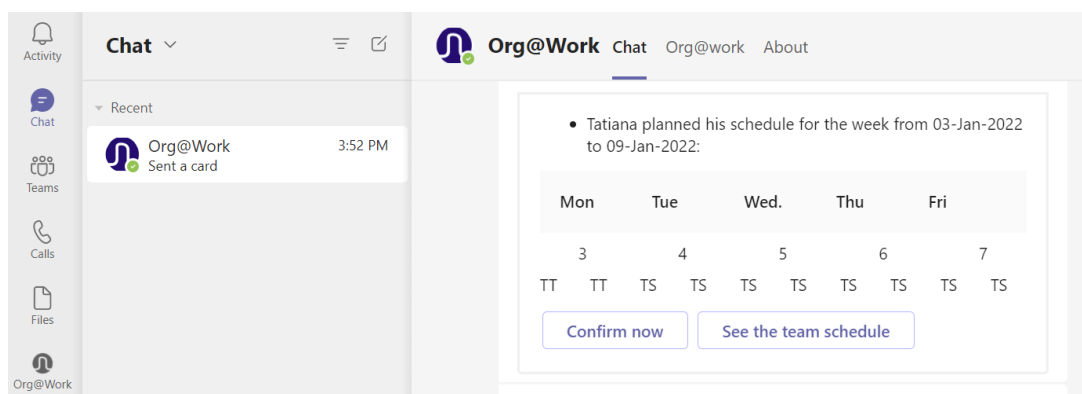
- Feedbacks & interactions withing a Team are facilitated by sharing permanently a given screen of your choice as a tab
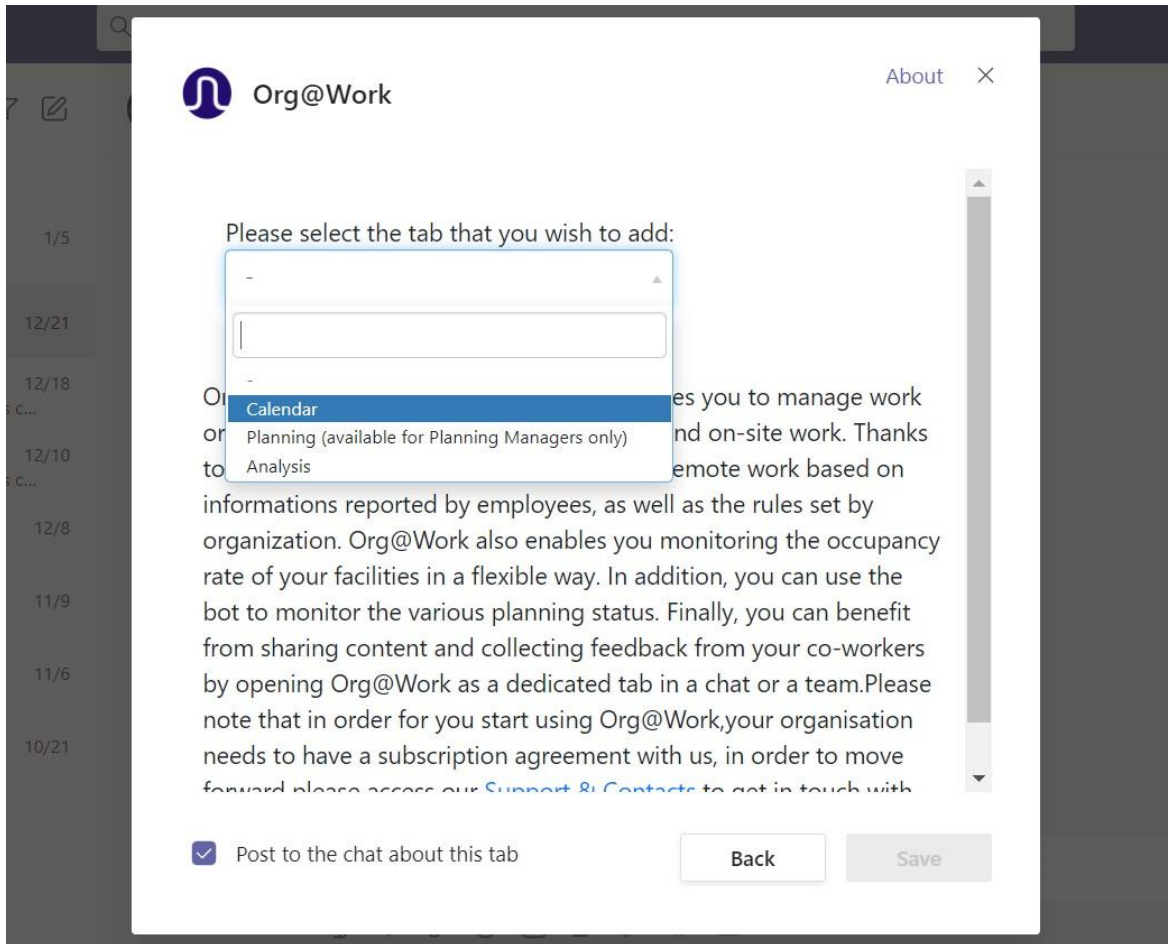
II. Support

Suggested escalation process

Aim of this process is to provide an accurate diagnosis of a given issue raised by the user, and thus avoid soliciting the Admin for a network issue that it will not be able to manage, for instance.
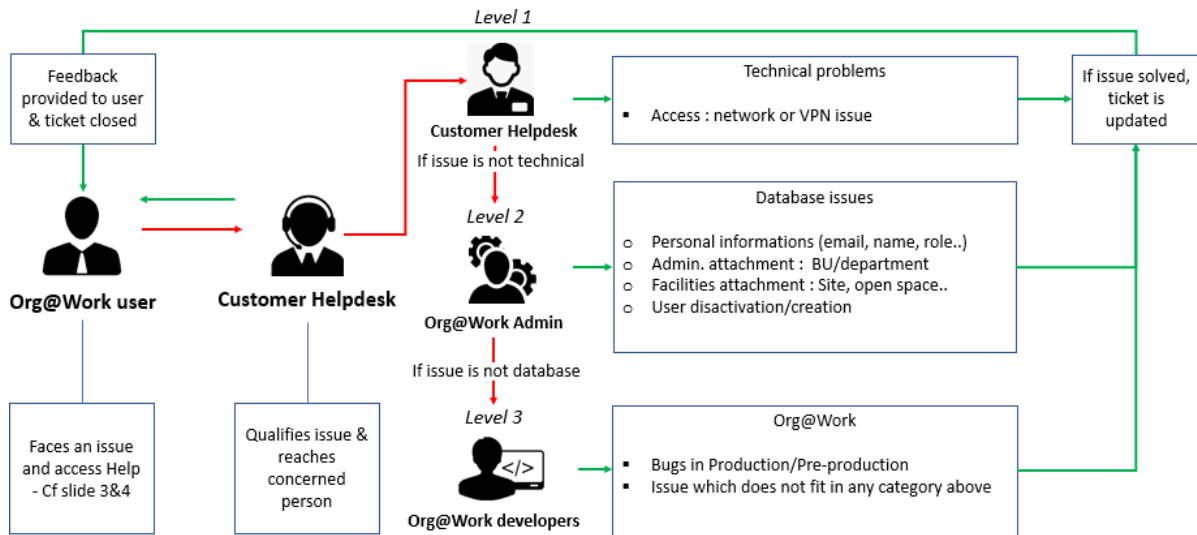
Pre-requisites

- Have an internal ticketing solution
- Create a dedicated Org@Work incident sub-category
- Provide hyperlink to be implemented on Org@Work 'Help' button

III. Technical focus

Authorized environment

| Technical overview	
Deployment environment	- Cloud (Azure, AWS..) - Client Premises (Windows Server 2016 or above) To benefit from encrypted communication between web server and browser, an SSL certificate can be incorporated to use https protocol
Database server	MSSQL Server 2016 or above To benefit from Transparent Data Encryption at rest, then MSSQL 2016 entreprise version is recommended or MSSQL 2019 standard/enterprise)
Development environment	Visual Studio 2019 Enterprise
Development language	ASP.net, C#, Web API under .NET Framework 4.7.2
Development libraries	Backbone js, jquery, bootstrap
Authentification	Mapping of Azure AD Client ID & Org@Work account

Org@Work as SaaS solution

Our SaaS integrates the Multi-Instance / Single tenant approach (single client) in which each client benefits from its own Org@Work instance, in terms of both Application and database. Benefits are:

- Better customization
- Greater control and own evolutions
- Better protection against security threats
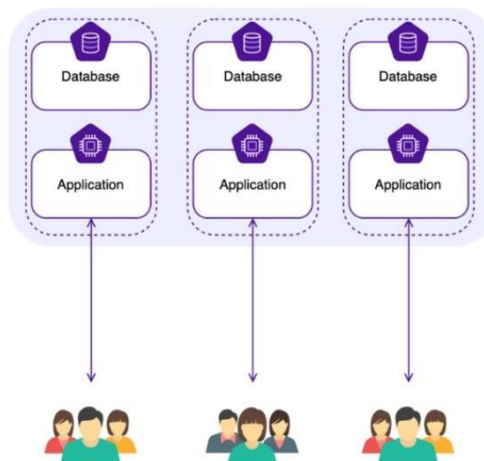
These instances can be part of cloud environments (ex :Azure, AWS…)

Hosting

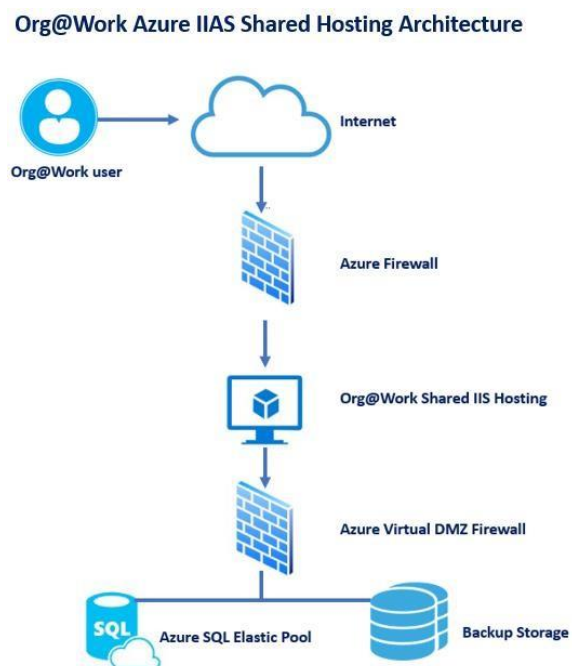### Recommended deployment environments

- Operating system: Windows Server 2016 or higher
- Database server: MSSQL Server 2016 or higher
- Servers required:
  - A server to support the production environment and its data
  - A server to support the pre-production environment and its data

✓ Compatible with deployments on physical / Cloud servers (Azure or AWS)
✓ Compatible with a SaaS deployment on Lundano's Azure Cloud

Lundano's Azure environment

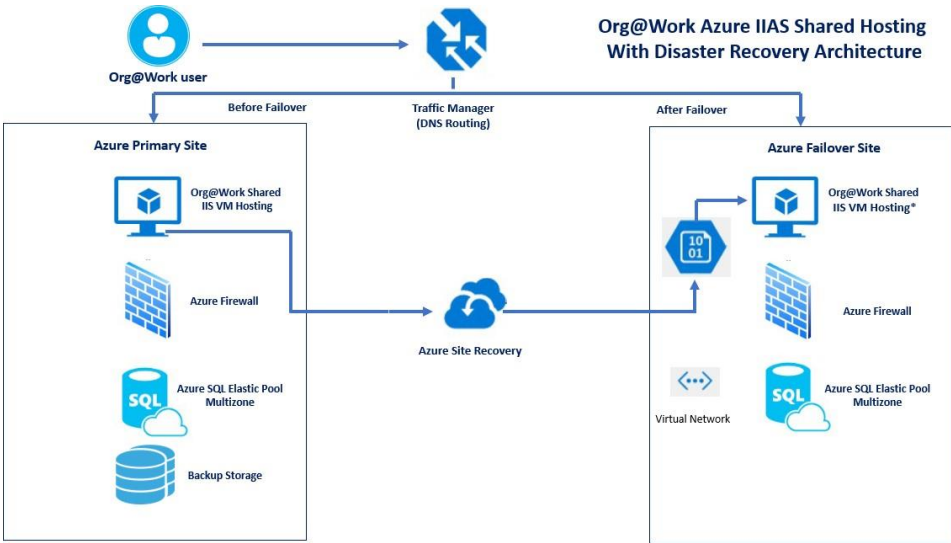Our model is based on a mixed **IaaS** (Infrastructure as a Service) approach for Web Application hosting and **PaaS** (Platform as a Service) for SQL database hosting.

- Web Application VM Operating system: Windows Server

- Database server: Azure SQL Database Elastic Pool
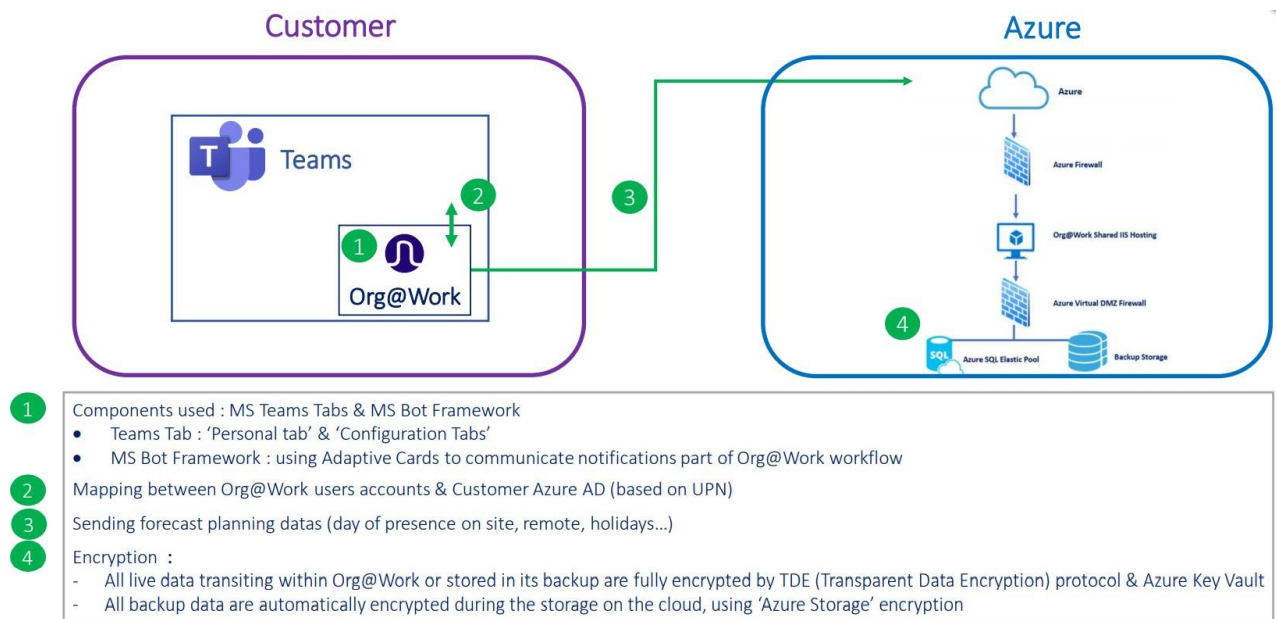
Azure architecture diagram

Org@Work Azure IIAS Shared Hosting Architecture

On demand – integrate a Disaster Recovery Plan strategy

Security

Overview

1. Components used : MS Teams Tabs & MS Bot Framework
   - Teams Tab : 'Personal tab' & 'Configuration Tabs'
   - MS Bot Framework : using Adaptive Cards to communicate notifications part of Org@Work workflow
2. Mapping between Org@Work users accounts & Customer Azure AD (based on UPN)
3. Sending forecast planning datas (day of presence on site, remote, holidays…)
4. Encryption :
   - All live data transiting within Org@Work or stored in its backup are fully encrypted by TDE (Transparent Data Encryption) protocol & Azure Key Vault
   - All backup data are automatically encrypted during the storage on the cloud, using 'Azure Storage' encryption

## Azure Services

- Once the Teams / Org @ Work application has been downloaded, the connection to services hosted on Azure is done in encrypted form (SSL).

- These services consist of:
    - Lundano control panel for validation of user tenant & client instance URL
    - Client instance
  ⇨ Control panel & Client instance are placed under Azure firewalls & Azure VNET

- Azure SQL Elastic Pool is secured thanks to :
    - Defender for SQL
    - Advanced data security for SQL Servers

Data encryption
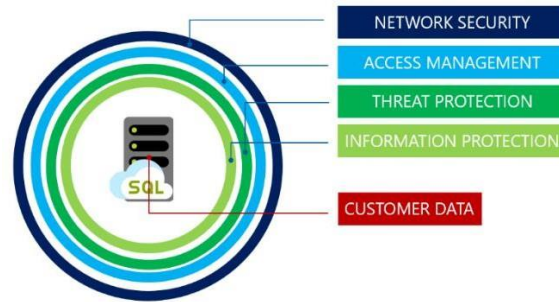
All data is encrypted via MS SQL, with 5 levels of protection

Live data

All data transiting live in Org @ Work (live) or stored in its backup is fully encrypted via the TDE (Transparent Data Encryption) protocol & Azure Key Vault

Backup

- All backup data is automatically encrypted during storage in the cloud, using "Azure Storage" encryption, reinforcing security & compliance commitments
- These inactive data are encrypted using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant
- In addition to encryption of inactive data, all backup data in transit is transferred over HTTPS, and always remain in Azure backbone network

Stand alone version specificities

Authorized browsers

- Microsoft Edge based on Chromium (latest version) on Microsoft Windows® 10
- Mozilla Firefox (latest version) on Microsoft Windows® 8.1, Microsoft Windows® 10
- Google Chrome (latest version) on Microsoft Windows® 8.1, Microsoft Windows® 10

Authentication though SSO

Customer is offered several authentication schemes for users' login to Org@Work. The list below shows the different supported protocols. Additional authentication schemes can be added at the customer's request.

Network-based

- Authentication with LDAP vs Active Directory Client.
- Requires user to provide user ID & password in Org@Work login page
- Customer must provide LDAP URL for Active Directory
  - ⇨ Recommended for use only under VPN network.

Based on an IDP

- Authentication using federated services (SAML 2.0)

- User authenticates on the client network, then is redirected to Org@Work with a SAML response including the authentication status, as well as additional fields to identify the user (such as the UPN or e-mail address)

- Customers must be able to provide:
  o An Active Directory instance where all users have an email address attribute
  o An installed and configured ADFS server
  o An SSL certificate to sign your ADFS login page and the fingerprint of the certificate.
  o Configure the AD FS server to add a relying party to Org@Work SSO login page with required request elements (UPN or email address)