

Appendix 3: Current ICT landscape

This appendix contains an overview of the current ICT landscape.

Datacenters

- The self-hosted services are offered from two on-premises data centers and the Microsoft Azure data center.

Network

- The Fontys on-campus network consists of a wireless and a wired network and is connected to the Azure network via an ExpressRoute.
- The on-campus network is connected to the Internet via the SURFnet network. Inbound and Outbound network traffic is regulated and inspected by a Cisco Firewall. From Azure is a direct link to the Internet. Inbound traffic to Fontys services in the Azure network goes through an Azure Firewall, Azure Application Proxy, Azure Application Gateway or an F5 BigIP (depending on the type of traffic). Outbound traffic from Azure to the Internet always goes through the Azure Firewall and is regulated and inspected accordingly.

Servers

- In total, there are approximately 275 servers, of which 200 are production servers (VMs). These production servers are distributed across the data centers: about 20% on-premises and 80% in Azure (IaaS).
- All servers run the Microsoft Windows Server OS.

Workplaces

- There are approximately 5,400 managed workplaces, of which about 90% are laptops and 10% are physical desktops and Azure Virtual Desktops.
- These workplaces are mainly used by employees of Fontys.
Students usually use an (unmanaged) private workplace (BYOD). Students do use the managed desktops or loaner laptops for educational purposes.

Applications

- Self-hosted applications: Fontys has about 235 self-built (web) applications that are hosted on the VMs or on Azure resources (PaaS).
- Cloud applications: The applications for Business Operations, Research and Education are now almost all cloud applications (SaaS).

- Workplace applications: Approximately 125 applications are offered at the workplaces of employees and students, through various application distribution methods. In addition, there are about 45 applications for management purposes (offered on Azure Virtual desktops).

Integration and Middleware

- For connecting applications and exchanging data, Fontys has developed its own Fontys Integration Platform (FIP) based on Azure resources (PaaS). Currently, FIP is also used to provision identities to a number of cloud applications.
- For internal applications, data exchange is facilitated by the Operational Data Store (ODS). This is a database with a large amount of (sensitive) information, such as telephone numbers, e-mail addresses and name and address details (including private ones).

Security

- For the security of all components in the data centers, for the workplaces, data and identities, the 'Microsoft Defender suite' and the SIEM solution 'Microsoft Sentinel' are used.

Identities

- Fontys has several types of identities that originate in 4 source administrations:
 - Employees in source system HR2Day (number 6,000)
 - Education participant in source system Progress (number 45,000)
 - Relationship in source system CRM (number 2,500) not in project scope
 - Non-personal in source system FAM (Functional Account Module) for functional accounts (number 600) and fixed global telephone numbers
 - A person can have multiple Fontys identities:
 - An employee who is also studying
 - A student who works as a student assistant for Fontys (employee)
 - A person has only one identity per type of identity.
 - An identity can have different accounts
 - MIM portal provides additional authorization to a business unit or department in case of a secondment.
 - The business model is the source administration for the Fontys organizational chart, the programs and the buildings.
 - The charging database is the source administration for the Fontys 06 number.

Identity and Access Management:

- For identity and access management, Microsoft Identity Manager (MIM) is used in combination with customization. MIM has multiple links to source and target systems.
- The main features of MIM are:
 - Automatically manage the lifecycle of an identity based on data from a source administration.
 - Automatically manage authorizations in the Active Directory based on attributes of an identity (business unit + department for employee, program + group for education participant).
 - Providing identity data to the integration platform (FIP), which in turn transfers this data to purchasing systems (ODS is a precursor to FIP, in phase-out).

- Creates the account, initial password, email address, landline phone number (employee and functional account only), and SIP address for communication purposes. In addition, it places the identity in a security group and distribution group based on the business unit and department (employee), or education and group (student). MIM also creates the necessary security and distribution groups, fueled by a user's business model and attributes, with the help of an external database called GroupsDB.
- Manages the lifecycle of an identity MIM with an external memory (delayed action database) to ensure the grace and retention time of an identity for graceful decay. MIM feeds the account communication database from which users receive messages about their account lifecycle (creation, end, renewal).
- The solution has a broader context, known as Enterprise User Management, in which additional functionalities are arranged:
 - A self-hosted self-service password reset solution, a forgotten password solution for students, a helpdesk solution for forgotten passwords, a self-hosted self-service email address change solution.
 - For interventions on the fully automated identity lifecycle process, a separate active directory instance, the Enterprise Directory Service (EDS), has been set up. This EDS has been expanded with the eduPerson scheme and contains additional personal data. Intervening actions include immediately disabling an account, removing a change date from an email address, and keeping an account alive longer outside of the delivery of a source system. The EDS also feeds the Fontys ICT University of Applied Sciences with employee and student data, they have a separate environment, the intention is to make this link to the new ICT solution.