Office 365 management done right

Delegate 365 White Paper

Authors: Toni Pohl, Martina Grom

Version: 1.5 of May 2017

For information about atwork pls. visit www.atwork-it.com .

For information about Delegate 365 pls. visit http://delegate365.com .

Content

Introduction

In Information Technology, we now face the ongoing popularity of cloud computing in many areas. Consumers as well as companies want easy to use and calculable services for basic infrastructure services like email, calendar and contacts with synchronization to many devices with different operating systems and form factors. In the field of enterprises collaboration platforms are replacing the long-term used sending attachments per email and enable content-management, sharing of documents and unified communication as well as social collaboration over corporate limits and continents. So the whole IT industry is beginning to change from local Client/Server deployments to Cloud Computing scenarios and solutions running in private and public datacenters.

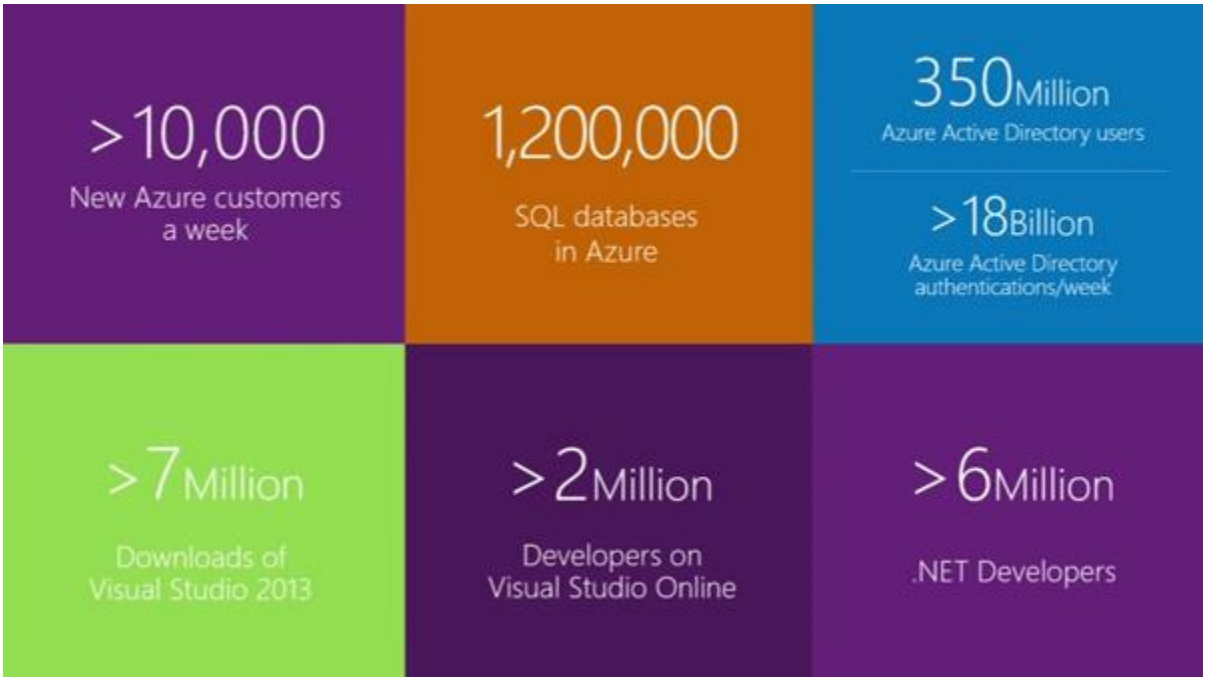
Of course, Cloud Computing increases security concerns for many companies and users. To ensure that their content is secure the cloud providers like Microsoft, Google, Amazon, Salesforce, Apple and so on are offering services based on secure standards. These providers take a lot of effort to security management. Consumer can benefit from the secure processes and standards but also need to take care about what information we put into the cloud. Going this way each company should have their individual rules about what data should be put where and what data must be encrypted or may not go into the cloud.

For many customers Microsoft Office 365 comes to use and replaces their own Email- or Collaboration-Servers. Especially hybrid-configurations make it interesting for medium to large customers to use the best of both worlds: private infrastructure combined with cloud services. In the Microsoft world tools like DirSync, ADFS or FIM enterprises can synchronize local Active Directories (AD) into the Cloud and provide Single Sign On (SSO) identity user experience and central identity management.

In IT-industry Microsoft is a leader in cloud security who implements policies and controls for their services. As of November 2014 Microsoft announced at the public Connect() event that the number of cloud users are steady increasing. To get an impression of the current numbers see the following screenshots taken from the event.

Microsoft Azure is generally available in 22 regions around the world, and has announced plans for 5 additional regions (as of 2016).

See the current list of Microsoft datacenters at http://azure.microsoft.com/en-us/regions/.
Microsoft handles more than 350 million AD users and more than 18 billion Azure Active Directory authentications per week. More than 80% of the Fortune 500´s are using services from Microsoft and it´s cloud services. With that numbers in mind we see that cloud business is real business and the trend of going into the cloud is definitely increasing.



Source: Microsoft, http://channel9.msdn.com/Events/Visual-Studio/Connect-event-2014/011

As we of atwork are using Microsoft cloud services since the beginning we have a lot of experience in consulting and caring about putting data into the cloud and creating web-services for various customers.

Our main focus is using Software-as-a-Service (SaaS) with Microsoft Office 365 and solutions around these services as well as developing individual solutions with Platform-as-a-Service (PaaS) with Microsoft Azure. We are a cloud based company and work close with and for Microsoft.

Office 365 is a great service to use from one person up to enterprises with ten thousands of users. Even if the management of Office 365 is easy the Microsoft Office 365 portal only allows a role based management for a whole Office 365 tenant. This means that for example a password admin can reset passwords of all users, not only for a special group of users he´s responsible for and so on.

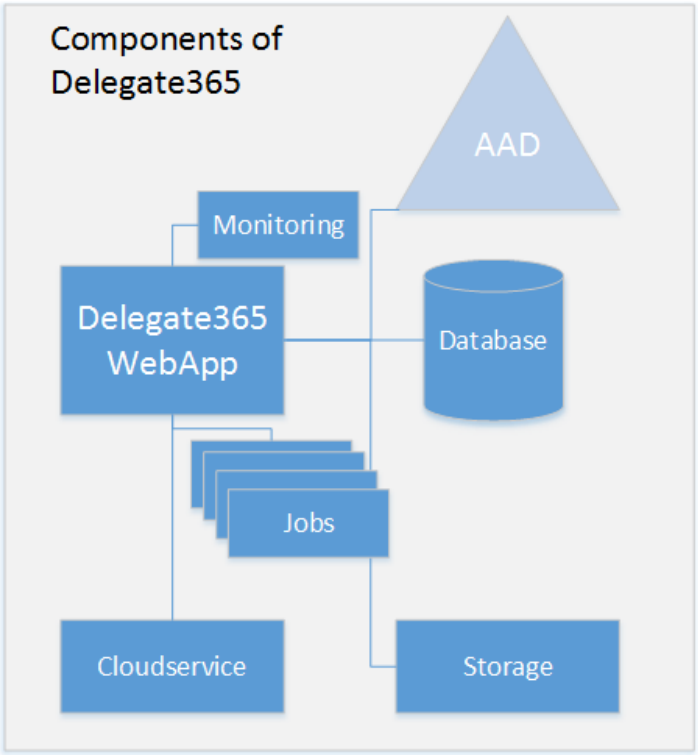
That´s where our product Delegate 365 (http://delegate365.com) comes in. Instead of using standard roles portal administrators can define any number of organizational units and who shall administer a logical unit and what licenses a unit can use. In Delegate 365 we call these units “Organizational Units” (OU) - like in Active Directory. A portal administrator controls who can administer what units and how many licenses are available for that unit. Reports show information about the usage. Delegate 365 also stores protocols of taken actions for later Auditing.

Delegate 365 adds functionality on top of Office 365 and works as an Add-On. Delegate 365 and Office 365 work absolutely together. There is no influence in the Office 365 services and users can still be created or managed in Office 365 itself. New or unknown users can easily be assigned to an organizational unit in Delegate 365. So Delegate 365 works as new standard portal with advanced management features and helps companies to meet their individual requirements and delegations.

Parts of Delegate 365–Solution Architecture

Delegate365 is a simple to use, web based portal for delegated user and license management in Microsoft Office 365. Delegate 365 consists of a web interface with a standard SQL-database and one (or many) cloudservice(s), depending on the version and the scenario. It interacts with Office 365 over API-calls via REST. All requests are secured by HTTPS and AAD-Authentication.

The Delegate 365 solution architecture looks as follows:



- **Delegate 365 web interface**. The web interface is an Azure App Service and is the interactive user interface for all admins. Only Delegate 365 admins have the right to login here with their personal Office 365 login. The portal admins define the group of admins. This portal replaces the Office 365 portal for standard user management. Each customer gets his own website.
- **Delegate 365 Microsoft SQL Server database**. The SQL database is running on an Azure SQL Database, see http://azure.microsoft.com/en-us/services/sql-database/. Delegate 365 stores user object IDs and group memberships in a relational database. The entity model is also represented in the Delegate 365 models and uses IDs for dependencies. Each customer gets his own database.
- **Delegate 365 cloud services**. This is the counterpart for special operations against Microsoft Exchange Online and is running as an Azure cloudservice. It´s the interface for actions that cannot be run in the Azure website because of technical or performance reasons. With version 2 and up the cloud service is part of a Delegate 365 instance.
- **Delegate 365 jobs**: These components run at specified times and execute synchronization, statistics and log operations. Log data is stored in a central Azure Storage and can be used with Storage Explorer or directly with Excel or Microsoft Power BI.
- Optional there exists a **Delegate 365 API** which can be consumed by other webservices, for example for external systems which want to create, update or delete users in Office 365. The Delegate 365 API is not part of a standard Delegate 365 instance and not described here. For more information about the API interface pls. contact atwork.

Platform

As Delegate 365 is used as SaaS, the platform itself also runs in the Microsoft cloud on Azure. Microsoft Azure offers reliable, enterprise grade infrastructure to securely host web sites and services with high availability by default.

Azure is the perfect platform for Delegate 365. Delegate 365 runs as Azure Website and as Azure Cloudservice. See http://azure.microsoft.com/en-us/ for further information on that platform.

Delegate 365 uses Azure Website Configuration settings and Azure SQL Database as storage. Microsoft provides Azure SQL Database as a standard service with integrated security and high availability (99.9%) with two replicas built-in for every SQL database regardless of edition. With Azure SQL Database there is no need for patching and OS updates and maintenance. See http://azure.microsoft.com/en-us/services/sql-database/ for further information on Azure SQL Database.

The standard hosting and services costs are included in the price of the Delegate 365 package.

If a Delegate 365 customer needs extra performance or has special requirements in availability, Backup or Restore plans or services these can be specially defined and regulated.

Built-in security

Delegate 365 is provided as SaaS and hosted in Microsoft datacenters. For information about security in Microsoft Azure see the Azure Trust Center at http://azure.microsoft.com/en-us/support/trust-center/.

atwork specified this software product for use in the cloud and secured all communication and data storage with modern industry standards for such services. Delegate 365 does by default not store any personal sensitive data in its storage systems.

Isolated customer data

Each customers gets his own instance of Delegate 365 with his own portal website and his own SQL database. This customer instance is created by atwork after the purchase is made. All configuration data is stored in the secured Azure configuration. Customer data is stored in the individual SQL database.

In Delegate 365 the data belongs to the customer. Customer data (see Personal data) is never mixed and always an own instance in Azure and SQL Azure. With that in mind it´s easily possible to backup, delete or restore all data of one customer without influencing any other customer service, instances of Delegate 365 are completely separated.

Operations

Delegate 365 communicates with the Microsoft Azure Active Directory (AAD) and Exchange Online. All data like user objects, groups or licenses are requested from the Microsoft API via secure HTTPS calls and from Exchange Online. So, all user and group details (user properties) are each time requested from the secure AAD service and are never stored in the Delegate 365 database, see below.

All writing operations are made directly in AAD or Exchange Online. This means that actions done in Delegate 365 are immediately visible in AAD/Office 365. If a writing operation fails for some reasons, the admin gets a notification with the error and each error is also logged into the audit log.

Reading operations in lists are usually getting data from the Delegate 365 cache layer. This is necessary to get a good and fast user experience since it would take too long to request data from Office 365 each time (especially for lists). Once an item is edited or accessed, Delegate 365 reads the corresponding data directly from AAD or Exchange Online and shows them in the task pane or in the view or edit page.

Personal data

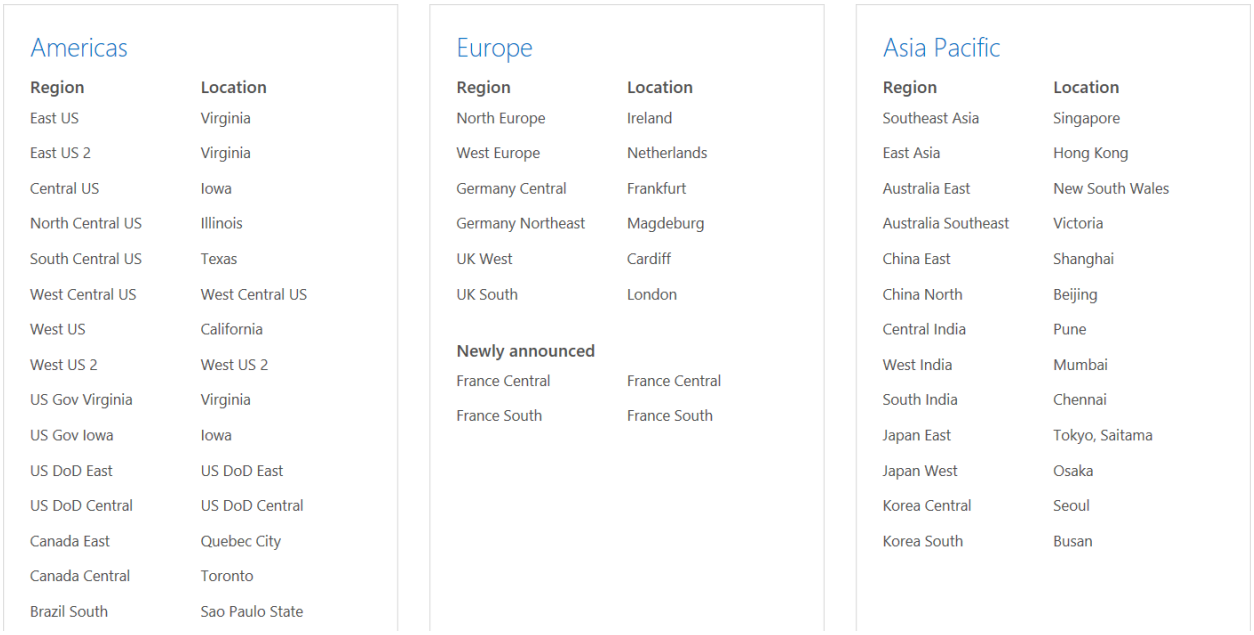
Delegate 365 just holds data about the organizational units (OU´s), consisting of the name and their IDs or GUIDs as well as the UPN of the administrators and user UPN´s. User UPN´s and some user properties and object GUIDs are stored in combination with Group-IDs to store relationships or to increase the performance which is used for caching purposes only.

IDs are simple numbers like 1,2,3 etc. Global Unique Identifiers (GUID) are long combinations of numbers and characters like 0240FD1B-0CA7-41BF-B92A-991EB51D8FC5. IDs are internally used for the identification of records and relationships between the tables.

Delegate 365 does store information about user actions like which admin created, edited or deleted a user object or assigned a license. These protocols can be accessed by the portal administrator for all actions or by the standard admins for their own actions and can be used for Audits.

Hosting

The hosting takes place where the customer wishes. As of today, these Microsoft Azure datacenters can be chosen:



Americas

Region	Location
East US	Virginia
East US 2	Virginia
Central US	Iowa
North Central US	Illinois
South Central US	Texas
West Central US	West Central US
West US	California
West US 2	West US 2
US Gov Virginia	Virginia
US Gov Iowa	Iowa
US DoD East	US DoD East
US DoD Central	US DoD Central
Canada East	Quebec City
Canada Central	Toronto
Brazil South	Sao Paulo State

Europe

Region	Location
North Europe	Ireland
West Europe	Netherlands
Germany Central	Frankfurt
Germany Northeast	Magdeburg
UK West	Cardiff
UK South	London
Newly announced	
France Central	France Central
France South	France South

Asia Pacific

Region	Location
Southeast Asia	Singapore
East Asia	Hong Kong
Australia East	New South Wales
Australia Southeast	Victoria
China East	Shanghai
China North	Beijing
Central India	Pune
West India	Mumbai
South India	Chennai
Japan East	Tokyo, Saitama
Japan West	Osaka
Korea Central	Seoul
Korea South	Busan

You can find a list of Microsoft's worldwide datacenters at http://azure.microsoft.com/en-us/regions/.

Microsoft also offers Azure Government, the cloud platform designed to meet U.S. government demands. For details see http://azure.microsoft.com/en-us/features/gov/.

Communication

Delegate 365 interacts with Office 365 over API-calls via REST (Representational State Transfer).

All requests against its own services and against Microsoft´s AAD or Office 365 APIs are secured through SSL transport layer. The portal website itself is also secured by HTTPS. Internally Delegate 365 does not use ASP.NET web forms but the modern way of ASP.NET MVC and async Javascript libraries, all secured by HTTPS.

The used HTTPS certificate (https://*.azurewebsites.net/) is provided by Microsoft for Azure websites by default. Optional custom certificates can be used but must be bought extra and be installed by the solution provider.

For the communication with AAD Delegate 365 uses a service principal (SPN) against the Microsoft APIs. The SPN is automatically generated by the setup of Delegate 365 and is valid for one year. After the setup wizard has created this service account the portal can be used for the configuration of the scenario. atwork takes care about the renewal of the SPN each year so that the service is available continuously.

Availability

By default, Delegate 365 runs on Microsoft Azure on the App Services platform and as cloudservice on a single core. If the Microsoft AppFabric reinstances a new machine there may be a downtime for up to about 15 minutes till the service is up and running again. This can happen from time to time by automatic processes in the Microsoft datacenters. As Delegate 365 is a user management tool a potential downtime is usually not business critical. The Azure SQL Database works internally with two replicas and should always be available. In our experience, such downtimes hardly happened but are possible from time to time. See more about Azure Service Level Agreements at http://azure.microsoft.com/en-us/support/legal/sla/.

If a customer needs higher availability the Delegate 365 services can be run in more cores so that there´s higher availability. This results in higher hosting costs. Pls. contact atwork for such scenarios.

Backup and Restore

As Delegate 365 is running on Azure as SaaS solution there´s usually no need to take care of backup and restore scenarios on the customers side because the services itself are designed to be up and running 24/7.

In case of deletion or any other destruction atwork reinstalls the services for the Delegate 365 customer with the latest service release of the Delegate 365 web and cloud service and with the latest backup of the Azure SQL Database in the Azure cloud.

Users, Groups and Licenses are not stored in Delegate 365 but in Office 365. So a potential data loss of Delegate 365 in the worst case – if the data restore is not possible for unforeseen reasons - means only that the organizational unit membership or licenses quotas and user action protocols are gone. In any case Office 365 users can continue to work as usual.

Anyway, if a customer wants to ensure a recurring (local or cloud) backup set of the Delegate 365 database itself pls. contact atwork for defining such an individual, fitting scenario.

Hybrid

Delegate 365 can manage users in the cloud (AAD). Despite of that Delegate 365 works with hybrid scenarios in the same way as the Office 365 portal. So, hybrid configurations are supported in Delegate 365.

Starting with version 2 of Delegate 365 synced domains and users are visible and group and license memberships are manageable. In Delegate365 the administrator can assign users to security groups and change the Office 365 licenses but cannot modify the user object itself because it´s managed in a local federated Active Directory. By now Office 365 and Delegate 365 cannot reach back into a corporate LAN

and carry out actions there. The sync action is working in the other direction, from LAN to cloud with Tools like DirSync, ADFS or FIM.

AAD handles federated objects differently, so these objects are no "full" objects with limited access in AAD which means they can be read but not changed. But with Delegate 365 administrators can change group and license memberships of such federated users.

As of 2015 Microsoft announced that next versions of DirSync can write back data from cloud (AAD) to local AD in hybrid scenarios. When this functionality becomes available, Delegate 365 will also be able to edit user data of local users (AD-users).

Concepts

Delegate 365 is for managing Office 365 users in medium to large organizations. The core concepts are simple: Delegate 365 works with Office 365 users, has two administrative levels and works with Organizational Units for the delegations within the organization.

Users

Delegate 365 is for administering Office 365 users (or any users in AAD) within the cloud. This means, any Office 365 user - regardless of any role in Office 365 – can be administered with Delegate 365 or can be a Delegate 365 administrator. There is no difference in administrators and users and there are no prerequisites necessary for users to act as Delegate 365 administrator – that´s one big difference between the Office 365 portal with roles and Delegate 365.

Administrators of Delegate 365 have to login in Delegate 365 portal with their personal Office 365 login and their Office 365 password.

The portal admin defines which admin is able to use what functions, like mass import users from a standard CSV-file, using Distribution groups, Shared Mailboxes and so on.

Security Groups

Delegate 365 can also handle group management. A portal admin defines which security groups can be used by which administrator. These memberships like in security groups can be relevant for example for using SharePoint Online portals or other apps which work with AAD. For delegation within Delegate 365 AAD security groups are not necessary.

Security Groups are synced when the Delegate 365 portal is opened or manually by the portal admin in the Sync-menu which comes starting with version 2.9.

Distribution Groups

The Delegate 365 portal admins define which administrator can create and manage own distribution groups within his management area. Distribution Groups are synced when the Delegate 365 portal is opened or manually by the portal admin.

Dynamic Groups

Dynamic groups can be managed with Delegate 365 as well. Administrators can define the rules to filter specific users by their properties or memberships.

Shared Mailboxes

The same concept as for Distribution Groups is available for defining which administrators can use Shared Mailboxes.

Rooms

The same concept as for Shared Mailboxes Groups is available for defining which administrators can use Rooms (resources).

Domains

Delegate 365 uses the domains from Office 365. This means, custom domains have to be added and verified in the Office 365 portal. Once custom domains are added, they are synced to Delegate 365 at the start.

The portal admin can also use the administrator dashboard to manually sync all data from Office 365 including newly added or deleted domains.

The portal admin also defines which admin can use which domains. With that definition an admin can only create or modify users for his entitled domains.

Roles

Delegate 365 only knows three types of users. Their admin membership is defined by the portal admin (who is the “master” of the Delegate 365 portal).

- Portal Admins
- Standard Admins
- Users*

“Admins” (Portal Admins and Standard Admins) get full access to the Delegate 365 portal. After opening the Delegate 365 web portal the standard login page of Office 365 follows. After successful login only Admins get the Delegate 365 portal site.

* (Non-Admin-) Users get a simple “Access denied” page for the Delegate 365 portal. There are special URL´s which are available for end-users, like the self-service password reset page and the user notification form page. That´s functionality coming with version 2.9 for giving end-users the possibility to change their self-service password reset data and performing this function to reset their password with Delegate 365.

OU´s

Organizational Units (OU´s) are soul of management in Delegate365 and represent any logical business unit, department or any other group. The rules are simple:

- An OU is a simple string, like “HR”, “IT-departement”, “Sales”, “Seattle”, “Paris”, etc. OU´s can be renamed anytime at will.
- The portal administrator defines any number of organizational units (OU) to create individual groups within the portal administration.
- Each administrator belongs to one or more OU´s (1 : n). This membership defines which OU´s he can administer.
- All user objects also belong to exactly one OU (1 : 1) to keep the management really simple.
- Objects can be moved from one OU to another OU with a mouse click.
- To keep this concept very simple there´s no nesting of OU´s available. The OU list is a flat list which can be reorganized easily by the portal admins.

Tip: With version 2.9 the Sync function can use predefined rules to put users automatically into a specific OU if a special user property (like Usage Location, Country, Department) is set or if the user belongs to a security group which is found in the OU list. With that settings new users can automatically assigned to an OU without any manual effort.

Licenses

If an Office 365 tenant is administered with Delegate 365 the portal administrator can define which admin gets which licenses and how many of them. Delegate supports license management and two license quota scenarios: soft limit and hard limit.

With soft limits an administrator gets an information about the used licenses but can overrule them by assigning licenses he usually doesn´t have within his OU. If hard limit (a flag called “enforce”) is configured the admin only can use the number of licenses that are predefined for his OU. So, Delegate 365 can help companies to limit the number of available and used licenses.

Also Delegate 365 offers a simple license order process for admins to request new licenses within the portal from their portal or license administrator. The license administrator then takes care of the ordering process (outside of Delegate 365), buys licenses which then are available in the Office 365 portal. From that point on these new bought licenses can be used in Delegate 365.

Each Delegate 365 customer can use the license management but must not.

Features

Delegate 365 addresses a lot of features for simplifying user management of Office 365 users, groups, Exchange functions, domains and licenses. The core features of Delegate 365 can be summarized by these functions.

- Delegate 365 is an own web portal which eases the whole user management of Office 365 users and offers a delegated administration.
- In Delegate 365 the delegation is handled with Organizational Units (OU´s) for defining any logical zone or unit, like “Paris”, “London”, “IT-department” or similar.
- Each user belongs to exactly one OU. Administrators can belong to many OU´s.
- The OU-concept is an add-on on top of the Office 365 users. The Microsoft Office 365 portal still can be used by IT-Admins.
- For managing new or unknown users (without any OU) in Delegate 365 they simply have to be assigned to a specific OU with a mass operation or automatic synchronization.
- Portal Admins can use the Sync function and settings for automatically assign new users and groups to a specific OU.
- Since users and groups are assigned to an OU, the responsible admins see these users immediately in their user´s or group lists.
- Users with the role “portal admin” define any number of other “admins” who shall be responsible for specific OU´s.
- Admins can see only users and licenses of their own OU´s as well as only use domains they are assigned to. The same happens with license plans.
- Portal Admins can rename the licenses and add metadata like costs or description and define a quota for each OU. This quota can be informational or can be mandatory so that each OU only receives a predefined number of licenses.
- Delegate 365 also provides often used Exchange functions like management of Distribution lists, Shared Mailboxes, Rooms, Contacts and user aliases.
- Admins can get information about all operations happened in Delegate 365 and about the number of users and licenses used via logs and reports.
- Self Service Password Reset (SSPR). Delegate 365 offers a password reset function for all users via E-Mail or SMS. Microsoft offers SSPR with premium features only. In Delegate 365 SSPR is built in. Costs for sending out Codes via SMS are additional (or bundled) depending on country and number of sent SMS, sending to E-Mails is free.
- Auditing. Each operation is protocolled in the Audit Log which can be filtered and exported to CSV or Excel-files by the Global Admins anytime.
- Notification Center. Support Cases, Messages from the Provider and Errors within the Delegate 365 are accessible anytime in the notification center in the upper right corner.
- Customization. Delegate 365 provides predefined color schemas and supports own logos.

The portal

Delegate 365 is an easy to use product and provides a fast web interface. Depending on your customer name the access to the website is usually https://<yourcompany>.delegate365.com (or a specific custom domain with SSL). You get this information from atwork after the setup process.

Delegate 365 can be preconfigured for your Office 365 tenant by atwork. Alternatively, the customer can do the binding of any Office 365 (or AAD) tenant himself with the two-step setup wizard in two minutes.

After the setup is done the first steps in the portal are to define OU´s and admins. From that point on the predefined admins can use the portal within their given OU´s to do user management. That´s it.

For information about the usage of Delegate 365 pls. have a look into the **Delegate 365 manual** and at the product website http://delegate365.com and see the screenshots and videos there.

Best practises

The Delegate 365 product website offers videos which show the first steps of doing the initial setup and the configuration for working with this product. See the videos at http://delegate365.com/videos.
The order of the videos reflects the recommendations and our best practices.

Resources

Pls. see the following resources for additional information about Delegate 365:

- http://bit.ly/d365web - the product website (in English)
- http://bit.ly/d365faq- see a list of frequently asked questions and answers
- http://bit.ly/d365videos - video tutorials for configuring the first steps
- http://bit.ly/d365-blog - see the latest updates online
- http://bit.ly/d365prices - see the prices for the default packages
- http://bit.ly/d365api - product website API page
- http://bit.ly/d365contact - product website contact form
- http://bit.ly/d365rssnews - changelog RSS feed
- http://bit.ly/d365blognews - blog changelog
- http://bit.ly/d365trial - Open a free trial with an Office 365 tenant
- http://bit.ly/d365overview - get an overview
- http://bit.ly/d365whitepaper - this whitepaper
- http://bit.ly/d365manual - download the manual
- http://bit.ly/atworkbuy - open the buying portal for purchasing Delegate365

Version History

atwork started the specification of Delegate 365 in 2012 and the development in 2013 because of the frequent demand for such a product which interacts with Microsoft Office 365. For a version history of Delegate 365 pls. have a look online at http://bit.ly/d365-blog or consume the RSS feed from http://bit.ly/d365rssnews.

Conclusion

Businesses today need productivity services that help users to work from virtually anywhere. Cloud services like Office 365 provide these services at a reasonable cost. That´s why millions of customers use these reliable and secure services. Medium to large organizations or companies often need a finer gradation than the role-concept in Office 365.

That´s where Delegate 365 (http://delegate365.com) comes in. Instead of using the Office 365 role administration Delegate 365 provides a layer above the user and license management and adds functionality on top of Office 365. Portal-Administrators can define any number of organizational units and administrators who can manage only their units. Additionally, there´s more Exchange functionality, license management, auditing and reporting built in.

Delegate 365 is a secure system which does not store any personal information and communicates with the Microsoft Azure Active Directory where all data is stored securely. Delegate 365 works perfectly with cloud only and with hybrid scenarios and runs in Microsoft Azure as SaaS.

For questions about Delegate 365 pls. contact us via office@atwork-it.com.