



*With the new Active Outlook App it is possible directly from Outlook 2013 or from the Outlook 2013 WebApp to archive emails directly or to outsource to a storage system. Full functionality of archiving and retrieval of emails is possible as well as the search function from within Outlook's own search app. Areas or categories are setup in the default settings for Outlook Email archiving and groups can be further defined over which user-rights can be regulated. Additionally, the various definitions in the rules can summarize and regulate the storage and allow access to the archived or outsourced emails.*

## Active Repository and Active Migration Manager

As shown above the Active Repository Manager and the Active Migration Manager should be deployed in an environment which can facilitate this structure and allow connection with the Office 365 environment. In Germany and Switzerland hosted environments will be soon be available to host these infrastructures.

These infrastructures will be linked, with the highest level of security (SSL encryption), to the Office 365 cloud. Of course, the infrastructure provided can be deployed as an on-site solution.

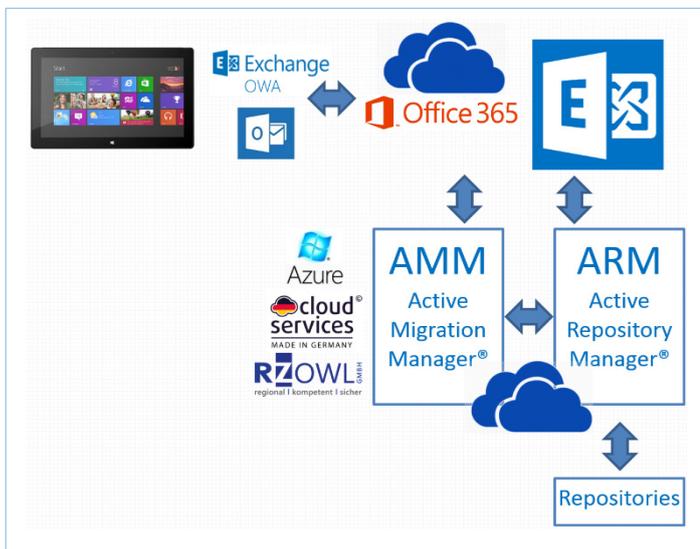
## Connection to Tamper-Proof Storage Systems

The existing Hosting Infrastructure offers a connection to tamper-proof storage von Iternity. iCAS (iTernity Compliant Archive Software) is a flexible and economical software solution for the protection of critical business data. iCAS ensures the integrity and availability of information from data management solutions (DMS/ECM, email, PACS etc.) irrespective of storage hardware. Archived data is protected from tampering and accidental deletion and checked for integrity. The patented ICAS technology offers tremendous flexibility and total integration into existing IT infrastructures. The procedure is tamper-proof and fully certified.

Again here, the highest level of security is standard both for network traffic and for storage and is always encrypted!

## Archiving Policies

Here different policies for the archiving of emails etc. are defined - initially, the name of the policy,



## The Architectur

The relevant processes and services such as ARM and AMM and the storage system are housed in an outsourced environment. This environment can be implemented as either an on-site solution or over a hosted environment.





the repository (storage target) and the retention period.

The screenshot shows the SharePoint mail archiving interface. The top part displays the 'Einstellungen' (Settings) page for 'Archivierungsrichtlinien' (Retention Policies). It includes a table with columns for Name, Repository, Aufbewahrungsfrist (Retention Period), Geändert (Changed), and Geändert von (Changed by).

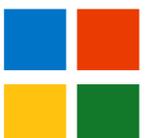
Name	Repository	Aufbewahrungsfrist	Geändert	Geändert von
10 Jahre	TestRepository	120 Monate*	20.12.2013 17:33:25	meissner@tecmast...
Keine Aufbewahrung	TestRepository		19.12.2013 15:36:32	meissner@tecmast...

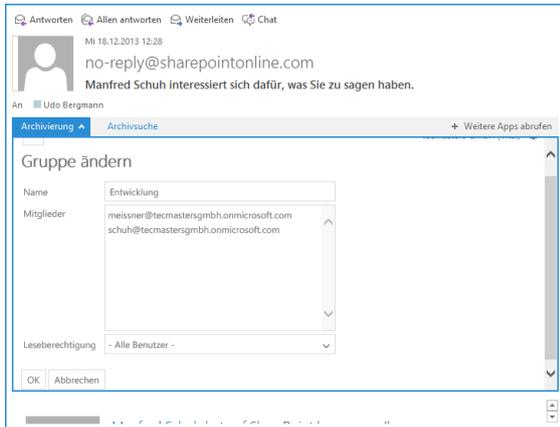
The bottom part of the screenshot shows a 'Richtlinie ändern' (Change Policy) dialog box. It contains the following fields and options:

- Name: 10 Jahre
- Repository: TestRepository
- Aufbewahrungsfrist: 120 Monate
- Ab Anfang des nächsten Jahres

## Groups

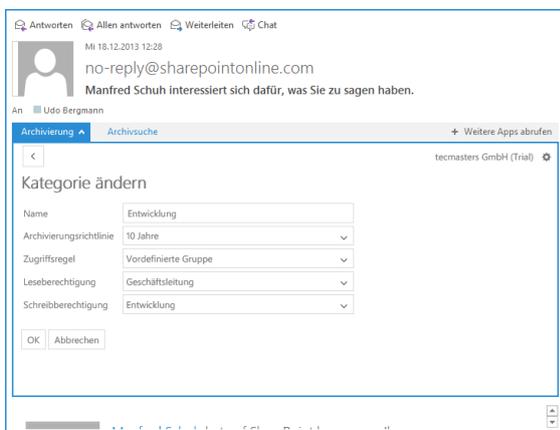
Creating mail archiving groups is fundamentally an organizational step. At this point groups are defined, for example, Development, Sales or Purchasing and the respective user rights are assigned for the users of each separate group.





### Categories

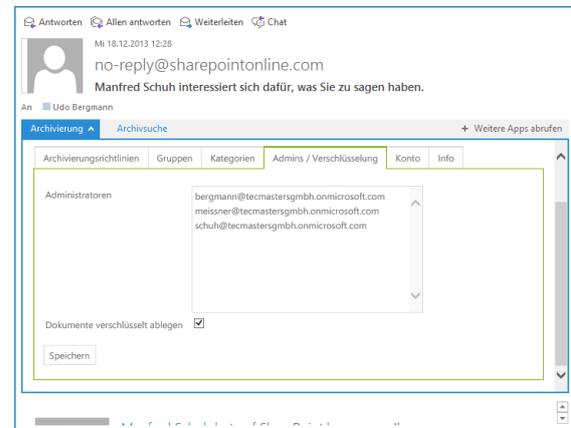
Categories are another organizational step where the administrator creates named categories, their relevant archiving policy and can associate, within this structure, previously defined rules. Alongside the pre-defined Group further access rules can be set parallel to the existing Group rights e.g. "The sender and recipient have access" or "Only the user who has filed the email" or "All have access" or the user can decide who will have access to the E-Mail. Of course, "Read permissions" and "Write permissions" can still be explicitly set for each created category.



### Administration – Data Encryption

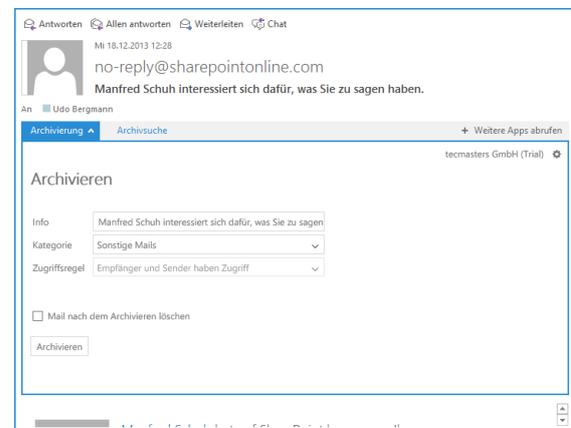
Administration und data encryption requirements for the system are setup by the

administrator. This includes settings as to whether the archived data (the Emails) for this Office 365 account should be encrypted or not. This means that the encryption is defined here for an organization not just for individual users.



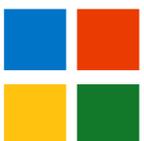
### Ad-Hoc and Automated Archiving

By accessing an archived email the administrator settings regarding permissions etc. will be implemented.



### Public Folders

A public folder in Office 365 Account can be setup in such a way that email within public

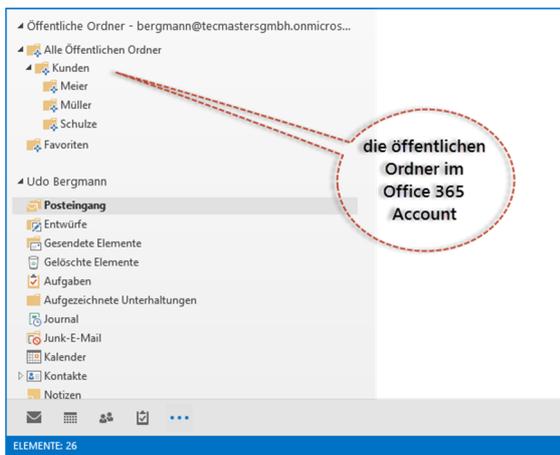




**Microsoft Partner**  
 Gold Hosting  
 Gold Server Platform  
 Silver Messaging  
 Silver Collaboration and Content



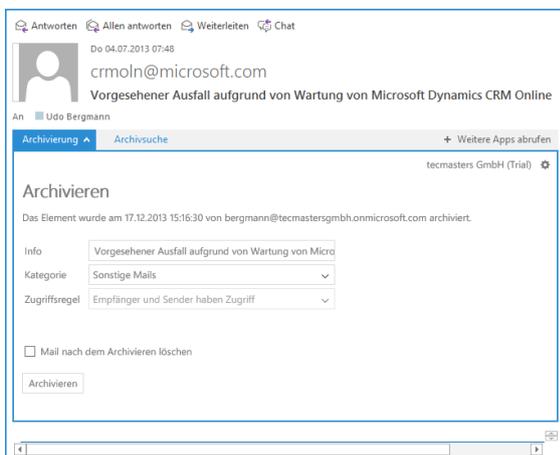
folders is automatically archived. It is also possible to define individual folders, or sub-folders to be archived. For the administration of Office 365 public folders, an account is required which has the necessary administration privileges.



## Archiving

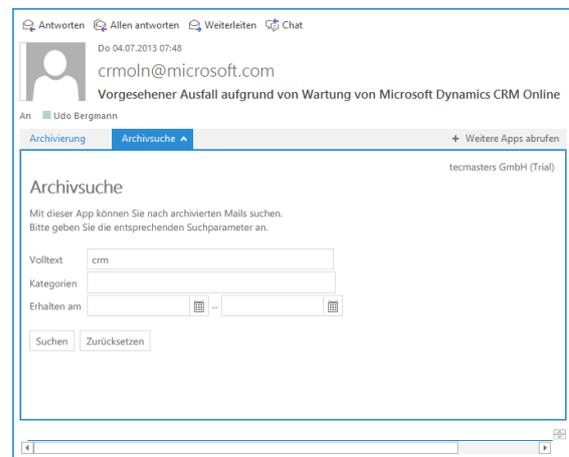
Archiving of email is easy to select within the preview pane. If required, the category and the access rules may be selected. The information is filled in automatically from the subject line in the email.

All relevant metadata relating to the email will be automatically archived.

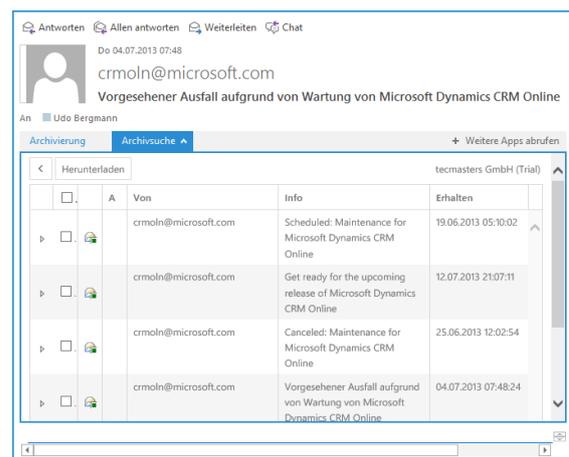


## Search

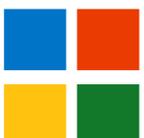
Almost all information in the email can be accessed by the full text search or filtered by using Category or Date as a search criterion.

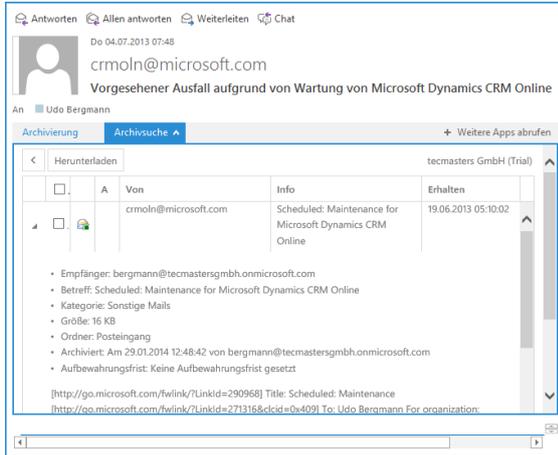


A hit-list displays all the emails found relevant to the search criteria.

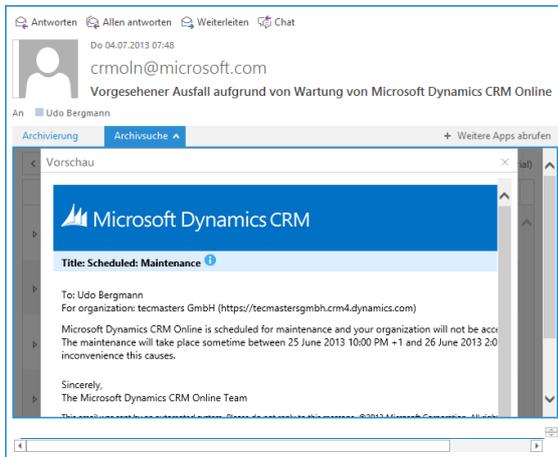


By opening the details for the hit-list entry the relevant meta-data concerning the email is displayed.





By clicking on the mail icon a preview can be viewed.



## PST Archiv Importer

The PST Archive Importer is an external utility. Utilities which allow email and structures which are archived in a PST file are therefore integrated in the search functions. Adequate user credentials and the necessary passwords are all that are needed to allow the access to the PST data and the relevant metadata e.g. the original folder and other metadata.

