Exchange in the cloud

Investigative and forensic aspects of Office 365

Owen O’Connor
Cernam Online Evidence

Intros

Focusing today on Exchange Online, the hosted Exchange component of Microsoft's Office 365 service offering

Why should we care about email?

- Exchange is one of the most important & sensitive stores of corporate records
- Also the repository of critical investigative data, e.g. mail content, user contacts, artefacts relating to email usage
- Often the focus of investigations, e.g., dealing with questioned records, unauthorised data access and data leakage / spillage

Why do I care?

Working with Exchange since the late 90's, beginning with Exchange 5.5
Pre Active Directory, pre LDAP, pre MMC!

Lots of IR projects, tons of investigations, too many e-discovery projects

Using and working with Office 365 and predecessor services since 2007

Plus, who doesn't love investigating email?

Understanding Office 365

Effectively two separate things

1. a set of Microsoft infrastructure products delivered as a service
2. a new way to purchase the Office application suite

We'll ignore the "way to purchase Office apps" piece and focus on 365 as a replacement for on-premises Exchange, SharePoint & Lync

- 3 core component services: Exchange Online, SharePoint Online, Lync Online
- Current version released this year but predecessor services date back to 2005
- Exchange Online is arguably the flagship service and the main driver for organisations migrating to Office 365
- Exchange Online is also available as a standalone service but in reality seems to be almost exclusively bought through Office 365 (e.g., to bundle Lync for IM)

What does Exchange Online give us?

Users get the full Exchange + Outlook experience, without the hassle of VPN for remote access, and with full mobile device support including ActiveSync and BES – practically no negative points

Administrators get **roughly** the functionality of Exchange 2010 for a fixed per-user cost, without the overhead of managing on-premises infrastructure for Exchange and AD and without managing backups, AV, spam solutions, etc

Security and DF teams get ... to live in interesting times

So, what happens if you encounter Exchange Online rather than Exchange Server in an investigation?

Administering Exchange

Exchange Online for administrators

Privileged users have two options for administering Exchange Online: a web console or a PowerShell remote session

The web console is really a collection of consoles: a top-level Office 365 console with basic settings for each service, plus product-specific consoles for Exchange, SharePoint and Lync

- Prior to the 2013 release the web console was a second-class interface and many common tasks required PowerShell
- Web console functionality is now far closer to parity and seems to be the main day-to-day interface for most O365 administrators
- As we'll see, several interesting investigative aspects **do** require PowerShell

Office 365 admin center

Cernam

dashboard
setup
users and groups
domains
licensing
service settings
service health
reports
support
purchase services
message center
tools

service overview

service health
2 issues

service requests
No open service requests

inactive email users
5 users have not signed in for 30 days or more.

mail protection
656 messages received, 93 blocked by filtering.

message center
1 new message in the past 7 days

current health

Exchange	Service degraded
Identity Service	No issues
Lync	Service restored
Office 365 Portal	No issues
Office Subscription	No issues
Rights Management Service	No issues
SharePoint	In extended recovery

view details and history

planned maintenance

07/10/2013 17:00:00 - Identity Service
Maintenance window: 5:00 PM UTC Monday, October 07, 2013 to 8:00 AM UTC Wednesday, October 09, 2013 Activities: Milestone Release Deployment Potential user impact: Isolated login failures are possib...
view details

view all

Search help and community

admin shortcuts

Reset user passwords
Add new users
Assign user licenses

resources

Working with domain names
Setting up mobile devices
Setting up user permissions in SharePoint
Office 365 Admin Help
Known issues
Information on Yammer

community

Ask a question in the forums
Check out our blog
Participate in the community

Exchange admin center

recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging

in-place eDiscovery & hold | auditing | data loss prevention | retention policies | retention tags | journal rules

Search the mailboxes in your organization for email and other message types that contain specific keywords. You can create a new search, or edit and restart an existing one. To update the search list, click Refresh below.

NAME	HOLD STATUS	MODIFIED DATE	CREATED BY
w	**No**	**04/10/2013 22:26**	**Admin**

W

Hold

None

Search

Status: Estimate Succeeded

Run by: Owen O'Connor

Run on: 04/10/2013 22:26

Size: 8.08 MB

Items: 146

Errors:
None

Statistics:
The keyword statistics table wasn't populated because the search query was empty.

Exchange Online versus Exchange Server

Exchange Online is effectively a subset of Exchange Server, mostly based on Exchange 2013 (but sometimes identifies as Exchange 2010)

Some aspects are identical to Exchange Server, e.g., the permissions model: mailbox level permissions, folder level permissions, SOBO, etc

Several key features which you may have used are unavailable, e.g., the "export-mailbox" and "get-logonstatistics" cmdlets

- Disabling certain features makes sense for a multi-tenant hosted service, **others …**

Overall Exchange Online feels familiar but remember that it is a “black box” cloud service where key functionality could change at any time

Audit trails

The bad news on audit trails

Moving to 365 means losing some of our most valuable data sources

- No authentication logs (really! forget about "who logged on around X time", "where did Y log on from this week“, "when did Z last log on" or even "how many failed logins have occurred for Z's account this month”)
- No client connection details (client agent, protocol, IP, computer name)
- No message tracking data
- No OWA webserver logs
- No details of last user logged on (“LastLoggedOnUserAccount” attribute)

Some data can **sometimes** be obtained indirectly from Microsoft Support

Some of these gaps can be filled through more complex hybrid deployments but the standard configuration causes significant issues

Cernam
Online Evidence & Investigations

So what **do** we get?

Microsoft provides 3 features which replace **some** of the missing data:

1. Mailbox Access audit trail
2. Admin audit trail
3. Canned reports

Mailbox Access audit trail

The mailbox audit trail includes details of non-owner access to mailboxes, e.g., admin access and delegate access

But ... auditing is **not** enabled by default, must be enabled **per mailbox**

- 3 key settings to consider in enabling auditing: AuditEnabled, AuditLogAgeLimit and AuditAdmin / AuditDelegate
- If auditing is not enabled for the **target** mailbox then **no events** are logged
- Microsoft support answers on "how do I do X for all users" can be ambiguous: appears to be no way to enable auditing globally, only for **then-live** mailboxes

Once auditing is enabled for a mailbox where do audit events get stored?

Mailbox Access audit trail

What's the craziest place you could think to store these audit events?

- Yup, **in** the target mailbox: when you access another user's mailbox, the record of that access is written into **their mailbox**, specifically in a folder named "Audits" under "Recoverable Items"
- Situation isn't quite as bad as it might seem: Exchange seems to effectively block access to the Audits folder **but** deleting the mailbox **does** delete audit data

Two options for viewing the audit trails: web console or PowerShell

- PowerShell gives significantly more detail via "search-mailboxauditlog" including client info: ClientInfoString, ClientIPAddress, ClientProcessName, ClientVersion

Bottom line: defaults are awful, most likely you will find auditing is not enabled and will need to enable it at the outset of your investigation

Admin actions audit trail

Admin audit log contains details of administrator actions other than mailbox access which result in changes

- i.e., ready only actions such as "get-*" cmdlet or browsing user config details are not logged
- Certain user events are also mysteriously logged, e.g., creating and deleting inbox rules

Admin audit log **is** enabled by default with a 90-day retention period

- No facility to configure or disable logging ("set-adminauditlogconfig" not available)

Audit events do **not** include client or source details

Cernam
Online Evidence & Investigations

Canned reports

Two reports with some value for investigations

1. "types of mailbox connections" (Get-ConnectionByClientTypeReport)
   Useful for spotting odd or unexpected types of access, e.g., POP3
   May be enough to warrant a support request to get detailed logs
2. Message delivery reports (Search-MessageTrackingReport)
   Accessible under Exchange admin center -> mail flow -> delivery reports
   View details of messages sent from or received by **individual mailboxes**
   Somewhat equivalent to the data previously found in message tracking logs but limited to single mailbox at a time and two week time window
   Get-MessageTraceDetail also useful, operates on 30 day time window

Accessing mailbox content

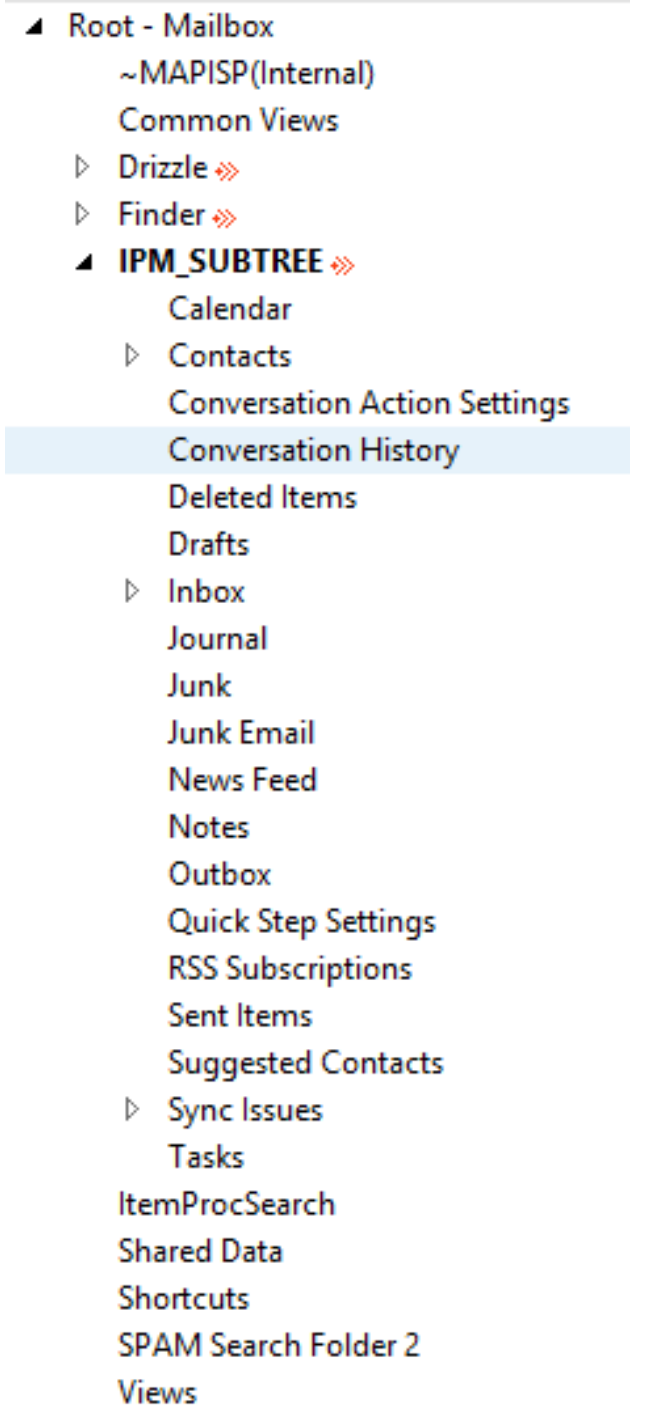
So you want mailbox content?

First question: **what content?**

- Just what you would see in Outlook?
- Do you need Dumpster content?
- Do you need folder associated items?

Dumpster content should arguably be part of every **investigative** mailbox export and time is a factor in obtaining Dumpster data

Associated items and other internal Outlook data can also contain valuable forensic artefacts



Cernam
Online Evidence & Investigations

Gaining access

Ideally we want to access a mailbox using delegated rights

- Any user can be granted full access to another user's mailbox (**without** granting them admin access to O365) via either the Exchange admin center or via PowerShell

Accessing mail data as the target user should be a last resort but could be done by obtaining or changing their password

Some OAUTH functionality also exists which might allow token-based access as a user, but documentation is patchy

Bear in mind: your access to the target mailbox may be audited and it may not be obvious who has access to that audit trail or if it is reviewed

Access mechanics

Using either delegated access or user credentials there are several routes to accessing mailbox data

1. Directly accessing the mailbox, using OWA or Outlook
2. Run a search using native tools and export the results
3. Export all mailbox content and search offline

Significant issues with direct access

- Covertness risks: read notifications, accidental changes, Lync presence integration, Out of Office reset, etc
- Search functionality has limitations and searches may be exposed to the user

Access mechanics

- Native search / ediscovery tools
  - Increasingly sophisticated "ediscovery" features including in-place search
  - All ediscovery features appear to rely on **indexed** searches (Exchange Search)
  - Exchange Search in on-prem servers needs care and feeding, e.g., to manage iFilters, re-index after adding iFilters, monitor non-indexed items
  - Exchange Search in 365 is a black box: can’t manage iFilters or re-index, can’t even see details of un-indexed content (no "Get-FailedContentIndexDocuments")
  - Have to assume that at least certain attachments or attachment types are not being indexed and potentially certain messages being missed entirely in indexing
- Bottom line is that the native tools (**if they are available**) are probably not the solution unless you would trust OWA search for an investigation

Access mechanics

- Leaving us … back in the 1990s: extract mailbox content and search externally
  - Likely the best approach for high-integrity search and for any investigation with multiple data sources, e.g., PC data as well as mailbox data
  - Multiple options for bulk mail access (MAPI, EWS, IMAP, POP3), each with its own issues, e.g., some will not provide MAPI-level properties, only SMTP headers
  - **Until recently** IMAP was a good starting point in terms of ease of use but now appears to no longer support delegated access ("user\target\password“ syntax)
  - IMAP, POP3 and EWS are non-native or second-class interfaces which work by translating a message from the native binary format to an RFC822-type format, causing issues with irretrievable items as well as generally poor performance
  - Certain third-party mailbox export tools are available but need to test carefully and consider interfaces used (e.g., IMAP cannot retrieve certain types of item)

The bottom line on mailbox access

Collecting “the whole mailbox” is probably impossible currently

- Even if you collect every user item – including calendar items, Lync conversations, tasks etc – you likely won't be able to collect all associated items, dumpster items or other internal content
- Certain mailbox content may not be available via any method, e.g., the mailbox audit information in the "audits" folder (remember: no backups available!)
- Even certain folders under IPM_SUBTREE may not be accessible via all interfaces, e.g., the various hidden folders under "Contacts" containing recipient cache entries, Lync contacts and Lync groups
- Lastly, even if you collect every item, are you collecting all of the metadata?

Looking in from outside

Detecting use of Office 365 externally

What if you don't have access or you're looking at another company?

Can we tell **whether** a particular company is using Exchange Online?

- Looking at "MX" records is obvious but not always accurate, e.g., a Microsoft MX may relate to FrontBridge anti-spam rather than Exchange Online
- SPF records for the domain are more accurate – query for "TXT" record and look for "**include:spf.protection.outlook.com**" or similar
- A "CNAME" named "**autodiscover**" pointing to autodiscover.outlook.com or similar is also a good indicator
- More generically an "NS" record for "**ORGNAME.onmicrosoft.com**" indicates that **some** O365 service has been provisioned at some point in time and an "A" record for "**ORGNAME-my.sharepoint.com**" points to Sharepoint Online

Cernam
Online Evidence & Investigations

Detecting use of Office 365 internally

Risk of unofficial Office 365 adoption is limited based on the requirement to verify domain ownership, similar to Google Apps

Internal clients could however be accessing personal O365 accounts, partner environments or unofficial corporate accounts on unmanaged domains

Unofficial use of O365 can be detected through DNS resolver logs or web access logs based on the following hostname artefacts:

```
lyncdiscover.*                  autodiscover-s.outlook.com
lyncdiscoverinternal.*          outlook.office365.com
webdir*.online.lync.com         pod*.outlook.com
sipdir.online.lync.com          *-my.sharepoint.com
```

Cernam
Online Evidence & Investigations

Investigating Office 365 users

If examining a dead system look for filenames ending “Autodiscover.xml” in Outlook’s local appdata folder

- Mailbox details
- Server details
- **Additional mailboxes** to which the user has access

At least in Outlook 2013 all mailboxes to which a user has full access are added to the MAPI profile by default, creating very useful artefacts

If investigating Exchange Online externally, check inbound mails for IP addresses included in an "**x-originating-ip**" header

Also be aware that Exchange Online supports SPF but currently **does not** support DKIM

Security considerations

Questionable Defaults

Although Office 365 is a great product there are some questionable security elements, beginning with the PowerShell admin interface

All users have access to the PowerShell remote session interface **by default**

Unprivileged users see far fewer PowerShell cmdlets but can run key commands like **“get-mailbox”** and **“get-mailboxstatistics”** against their own mailbox

Even with limited access an unprivileged user can view several sensitive items

- Litigation hold status and basic details of any hold
- Auditing status and configuration (including specific events for which auditing is enabled)
- SOBO permissions (but **not** mailbox-level permissions)
- Any deliver-and-forward config (as sometimes used for “double-delivery” monitoring)

Users can also view some tenant-level settings including the list of accepted domains (potentially reflecting new ventures, pending acquisitions etc)

Questionable Defaults

Newly-created Exchange Online mailboxes have **every** external interface enabled by default

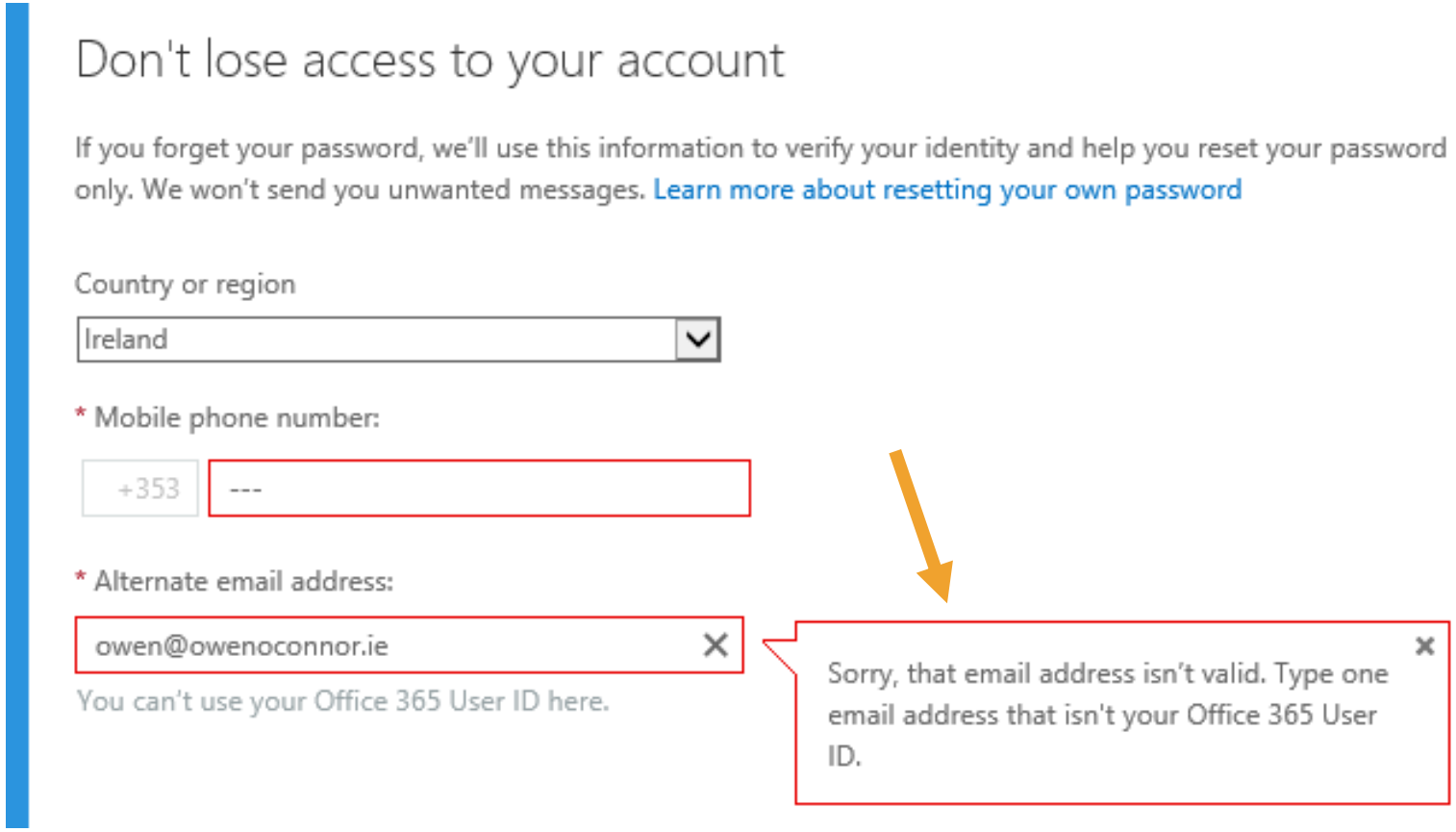
- MAPI
- OWA
- OWA for devices
- Exchange ActiveSync
- IMAP
- POP3 (including plaintext!)

By default there are no restrictions on addition of mobile devices, including via ActiveSync, i.e., any user can **add their own mobile** device, company-issued or not!

Administrative password recovery

Office 365 users with admin privileges can recover their own passwords

365's web console **strongly** encourages adding recovery contact details



Administrative password recovery

As well as nagging users on each login the 365 web console will refuse to add an admin role to a user unless recovery details are provided

365 refuse to accept secondary email addresses which are hosted within the same 365 organisation – must be external, e.g., Gmail

Microsoft then uses the secondary address for certain emails as well as for recovery purposes

Cellphone number is also required for PhoneFactor verification but not verified against any corporate contact details

Mobile device security

365 has (mostly) full Exchange ActiveSync support, including the ability to view the last successful sync time

- Can view full details of device make and model
- Can (sometimes) also see device IMEI and mobile network subscriber number

```
FirstSyncTime                 : 01/05/2013 20:25:05
LastPolicyUpdateTime          : 21/09/2013 00:14:36
LastSyncAttemptTime           : 06/10/2013 15:15:20
LastSuccessSync               : 06/10/2013 15:15:20
DeviceType                    : iPad
DeviceID                      : ApplDLXH
DeviceUserAgent               : Apple-iPad3C1/1101.501
LastPingHeartbeat             : 600
DeviceModel                   : iPad3C1
DeviceFriendlyName            : Black iPad
DeviceOS                      : iOS 7.0.2 11A501
DeviceOSLanguage              : en
DeviceEnableOutboundSMS       : False
IsRemoteWipeSupported         : True
DeviceAccessState             : Allowed
DeviceAccessStateReason       : Global
DeviceAccessControlRule       :
DevicePolicyApplied           : CERNAM.onmicrosoft.com\Default
DevicePolicyApplicationStatus : AppliedInFull
LastDeviceWipeRequestor       :
ClientVersion                 : 14.1
NumberOfFoldersSynced         : 15
ClientType                    : EAS
```

Mobile device security

Remote device wiping is a key part of Exchange ActiveSync and works well on Office 365 **from PowerShell**

- Device wipe commands can also be sent from the web console but in repeated testing we have never seen this work
- Wipes sent from web console seem to have no effect: device continues working, even continues to sync mails as normal
- Wipes sent from PowerShell take effect **instantaneously** in our testing

Device acknowledgement of wipe and final wipe status are both accessible through PowerShell and **should be checked** in all cases

Cernam
Online Evidence & Investigations

Finally on security

There are many other positive aspects we don't have time to cover

e.g., Microsoft's document-level DRM solution is also available as a service, and potentially of benefit in certain types of investigation

Bottom line: Exchange Online needs ongoing care and feeding

1. Enable auditing for all mailboxes and add to user provisioning process
2. Disable un-used or unauthorised interfaces (POP3!) for all mailboxes
3. Block users' ability to add own mobile devices, approve by exception
4. Extract and review key reports regularly (e.g., automate via PowerShell)

Questions?

Owen O’Connor

owen@cernam.com