Informazioni documento			
Cliente:			
Oggetto:	Security and Permission filtering on Office 365		
Creato da:	Francesco Pandiscia	**Data creazione:**	4/10/2016
Commessa:		**Rif.to Offerta:**	

Storico versioni			
Nr.	**Data**	**Autore**	**Descrizione**
1	4/10/2016	Francesco Pandiscia	Stesura iniziale del documento

Sommario

Indice delle Tabelle

1 INTRODUZIONE

1.1 Obiettivi

Il presente documento va a descrivere le modifiche implementate in ambito limitazione di permissions per il contesto Global Administrator di Office365, relativamente alle possibilità di Mailbox Search e di Mailbox Import/Export.

2 PERMISSIONS IN OFFICE 365

Per poter implementare le modifiche richieste è stata inizialmente effettuata un'analisi per verificare l'attuale implementazione dei privilegi lato Management Role di Office 365. Per poter semplificare il management della delega delle permission in modalità granulari sono stati dapprima creati due universal Security Group Mail-Enable nella AD On-Premise e una volta replicati tramite sincronizzazione della directory verso la Azure AD di 365, sono stati associati ai rispettivi ruoli RBAC.

In particolar modo è stato creato un gruppo "g_O365_EDiscovery" con la possibilità di effettuare delle ricerche cross-mailbox nell'intera organizzazione; mentre un secondo gruppo "g_O365_MB_ImportExport" è stato delegato alla possibilità di fare esportazione del contenuto mailbox in file PST. Sono stati quindi dapprima normalizzati i ruoli "Mailbox Import Export" e il "Discovery Management" e poi tramite connessione powershell verso il tenant 365, eseguiti i seguenti comandi powershell:

```
PS C:\Users\Francesco\Downloads> New-ManagementRoleAssignment -Role "Mailbox Import Export" -SecurityGroup "G_O365_MB_Im
portExport"

Name                           Role             RoleAssigneeName  RoleAssigneeType  AssignmentMethod  EffectiveUserNam
                                                                                                      e
----                           ----             ----------------  ----------------  ----------------  ----------------
Mailbox Import Export-G_O36... Mailbox Import... G_O365_MB_Impo... SecurityGroup     Direct


PS C:\Users\Francesco\Downloads> Add-RoleGroupMember -Identity "Discovery Management" -Member "g_O365_EDiscovery"
PS C:\Users\Francesco\Downloads>
```

Per la gestione operativa sarà quindi possibile gestire direttamente la group membership dei gruppi sopra citati, al fine di delegare le permission specifiche.

A seguire riporto il risultato di un report sulle membership dei ruoli built-in di 365; in giallo evidenziato gli utenti con diritti di Company Administrator ed Exchange Service Administrator, con diritti di amministrazione in ambito Exchange Online di 365.

Report Ruoli Built-In di 365 e relativa membership

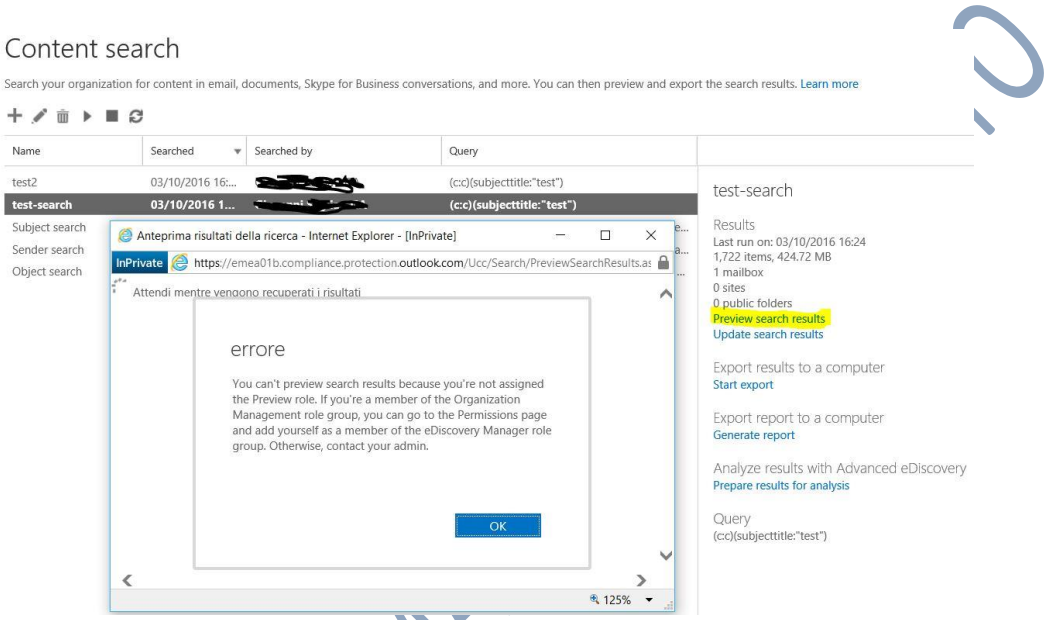
RoleName	DisplayName	Emailaddress
Billing Administrator	xxx - External	lorenzo.xxx@xxx.onmicrosoft.com
Billing Administrator Conteggio	1	
Company Administrator	xxxx Giovanni	giovanni.xxx@xxx.com
Company Administrator	xxxxx Giampietro	giampietro@xxx.com
Company Administrator	DirSync	DirSync@xxx.com
Company Administrator	Filippo Barsotti GA	Filippo.Barsotti-GA@xxx.onmicrosoft.com
Company Administrator	Giovanni Saglia - GA	Giovanni.Saglia-GA@xxx.onmicrosoft.com
Company Administrator	Barsotti Filippo	filippo.barsotti@xxx.com
Company Administrator	Gatti Davide - External	davide.gatti@xxx.com
Company Administrator Conteggio	7	
Directory Readers	Microsoft.Azure.AnalysisServices	
Directory Readers	Microsoft.YammerEnterprise	
Directory Readers	Reporting API Application	
Directory Readers	Microsoft.Azure.ActiveAuthn	
Directory Readers Conteggio	4	
Directory Synchronization Accounts	On-Premises Directory Synchronization Service Account	Sync_SYNC2_30252556e5e4@xxx.onmicrosoft.com
Directory Synchronization Accounts	On-Premises Directory Synchronization Service Account	Sync_ID0799_351891b3f2a6@xxx.onmicrosoft.com
Directory Synchronization Accounts Conteggio	2	
Exchange Service Administrator	Marinelli Antonio - External	Antonio.Marinelli@xxx.com
Exchange Service Administrator Conteggio	1	
Helpdesk Administrator	Rossi Massimiliano	massimiliano.rossi@xxx.com
Helpdesk Administrator	Biolzi Luigi	luigi.biolzi@xxx.com
Helpdesk Administrator Conteggio	2	
Lync Service Administrator	Sorrentino Serena	serena.sorrentino@xxx.com
Lync Service Administrator Conteggio	1	
Service Support Administrator	Biolzi Luigi	luigi.biolzi@xxx.com
Service Support Administrator	Sorrentino Serena	serena.sorrentino@xxx.com
Service Support Administrator	Veronainformatica	xxx@xxx.onmicrosoft.com
Service Support Administrator	xxx - External	lorenzo.xxx@xxx.onmicrosoft.com
Service Support Administrator Conteggio	4	
SharePoint Service Administrator	Xxx xxx	serena.xxx@xxx.com
SharePoint Service Administrator	Mario Verdi	mario.verdi@xxxinternational.com
SharePoint Service Administrator Conteggio	2	
User Account Administrator	Rossi Massimiliano	massimiliano.rossi@xxx.com
User Account Administrator	xxx	luigi.xxx@xxx.com

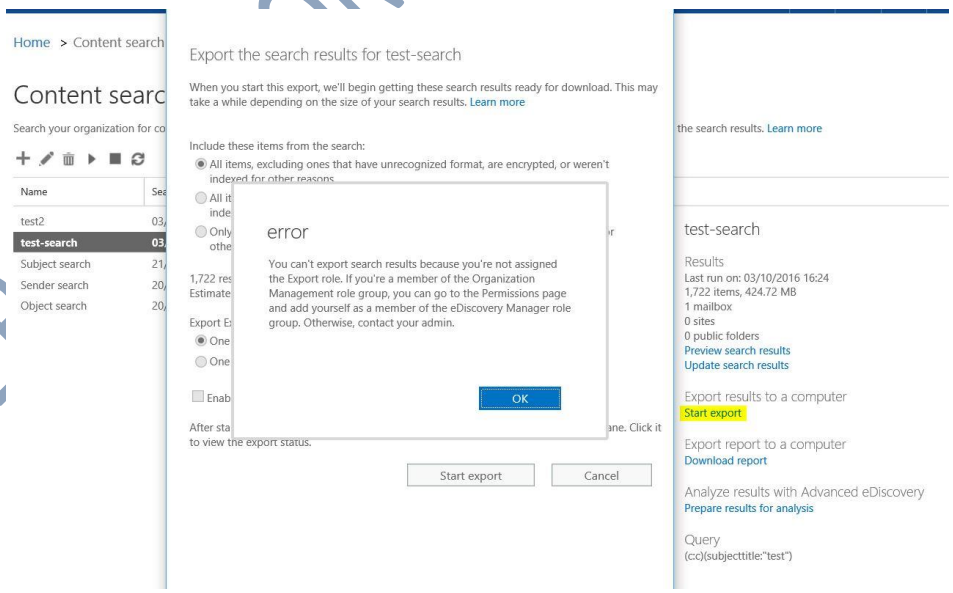
User Account Administrator	Sorrentinoxxx	serena.sorrentino@xxx.com
User Account Administrator Conteggio	3	
Conta comp.	27	

Tabella 1: Report MSOL Built-in Role Membership

Gli utenti sopra evidenziato potranno in qualità di amministratori della componente Exchange, creare nuove query di interrogazione dei contenuti sia per la parte di ricerca, che per la parte di "export", ma non potranno visualizzare, né salvare i risultati ottenuti.

ES:





3 CONCLUSIONI

La gestione delle permissions per quanto riguarda le operazioni di Search-Cross Mailbox ed Import/Export dei contenuti Mailbox, avendo impatti potenzialmente considerevoli in termini di privacy e security, è stata demandata alla membership di gruppi AD creati ad-hoc, in modo da poter gestire in maniera autonoma la concessione delle singole funzionalità.