Maximize Security in your Office 365 Matters

Daniel Pelc, Sr. Consultant Discovery Management

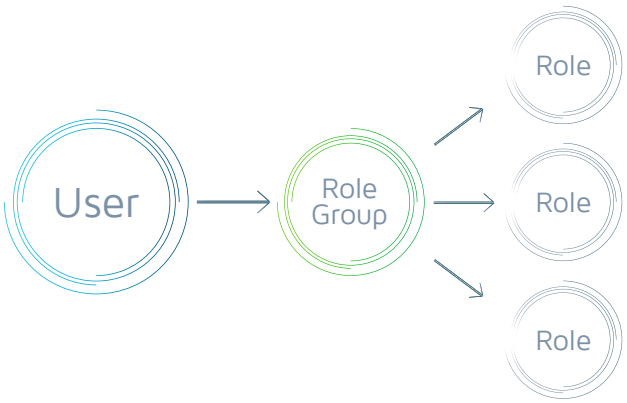
NightOwlDiscovery®

It's the secret vault behind the secret vault. What kind of corporate "treasures" are kept in Office 365 eDiscovery matters? Source code? Client lists? Supply chains? Wouldn't some people like to know? What would a bad actor do to get those gold nuggets? With more and more companies moving to Office 365, how much security is required to make sure the secrets stay secret? In the coming weeks, we will explore different strategies to maximize the security of Office 365 eDiscovery matters.

Office 365 is built with the corporate IT infrastructure in mind. The Advanced eDiscovery module, part of the E5 license, is built as an adjunct application to facilitate easy search, preservation and processing of key evidence. According to *Info Security Magazine*, 43% of data loss is caused by insiders. Half of that 43% figure was intentionally stolen. A logical step to prevent data theft is to only provide users with access to information that they need for their role. We're going to look at how several simple permissions control strategies can improve security across matters.

ROLES, ROLE GROUPS AND MODIFICATIONS

Roles in Office 365's Security and Compliance Permissions menu provide the right to perform or supervise a certain task. Office 365 groups roles together into "role groups." Individuals are assigned to a specific role group, which bundles together the roles that a user will need to perform their job. Although similar in function, the roles in the role groups may differ. Additionally, there may be different types of member sub-role groups in a role group, i.e. the eDiscovery Manager and eDiscovery Administrator are both members of the eDiscovery Manager role group, but have very different rights. The role groups are customizable by changing the roles assigned to each role group. However, Microsoft does not advise modifying the default role groups and instead recommends that users clone the role group and modify the permissions under a new name.



KNOW YOUR ROLES AND ROLE GROUP PERMISSIONS

Permissions for Office 365 eDiscovery are broken out by task/role across the specific user role group. The permissions for each role are based on a Role Based Access Control (RBAC) system. This model allows each user only the access they need to perform their tasks. In the permissions section in the Security and Compliance menu, each role group has a specific task-based security profile. In the permissions interface, each role group is listed on the left side and the roles found in each role group are listed on the right side under Assigned roles.

There is also a list of common user role groups and a permissions comparison found in FIG 1 below.

At the beginning of the case, carefully consider the following:

- How many role groups and roles will be required in your matter?
- How might the roles required by each role group change as the matter proceeds?
- What security risks does each role pose?
- What happens if a person in one of the role groups leave?

KNOW THE DIFFERENCE BETWEEN AN EDISCOVERY MANAGER AND AN EDISCOVERY ADMINISTRATOR

An eDiscovery Manager is the manager of cases created by or assigned to them. Managers control who can access the matter and are able to create holds and content searches. Matters not created by an eDiscovery Manager are invisible and inaccessible to that user.

An eDiscovery Administrator is similar to an eDiscovery Manager. However, they are able to view all matters across the organization and are able to assign themselves to manage any matter unilaterally. Although these roles are part of the same role group, the rights granted to each are drastically different. Be very careful who is assigned to the Administrator role group as they will have the keys to the kingdom. If only one person is assigned to that role group, the visibility across the organization's matters may be lost if they depart. There are several reasons why granting administrator access across matters makes sense.

- If one person is solely in control of a matter, solitary control means that no one else is able to access the matter. That individual is free to have access to any data in that matter without any checks. Should that individual leave, critical knowledge may be lost.
- The administrator is able to provide oversight across all matters and ensure that processes are followed appropriately.
- eDiscovery Managers may need a backup. By providing this level of access to the eDiscovery Administrator, tasks can be shared amongst members of the case management team quickly and simply.
- The eDiscovery Administrator is able to monitor suspicious activities across matters.

By correctly applying permissions across role groups and roles, an organization is in a much better position to prevent insider data theft. The first key to preventing a break in is to lock the front door.

FIG 1. Microsoft Common User Role Groups and Permissions Comparison

Role Group	Compliance Administrator	eDiscovery Manager & Administrator	Organization Management	Reviewer
Case Management Lets users create, edit, delete, and control access to eDiscovery cases in the Security & Compliance Center. For more information, see Manage eDiscovery cases in the Office 365 Security & Compliance Center. As previously explained, a user must be assigned the Case Management role before you can use the **Add-eDiscoveryCaseAdmin** cmdlet to make them an eDiscovery Administrator.	YES	YES	YES	NO
Compliance Search Lets users run the Content Search tool in the Security & Compliance Center to search mailboxes and public folders, SharePoint Online sites, OneDrive for Business sites, Skype for Business conversations, Office 365 Groups, and Microsoft Teams. This role allows a user to get an estimate of the search results, but additional roles are needed to perform actions such as previewing, exporting, or deleting search results. For more information about Content Search, see Run a Content Search in the Office 365 Security & Compliance Center.	YES	YES	YES	NO
Export Lets users export the results of a Content Search to a local computer. It also lets them prepare search results for analysis in Advanced eDiscovery. For more information about exporting search results, see Export search results from the Office 365 Security & Compliance Center.	NO	YES	NO	NO
Hold Lets users place content in mailboxes, public folders, sites, Skype for Business conversations, and Office 365 groups on hold. When content is on hold, content owners will still be able to modify or delete the original content, but the content will be preserved until the hold is removed or until the hold duration expires. For more information about holds, see Manage eDiscovery cases in the Office 365 Security & Compliance Center. Overview of retention policies	YES	YES	YES	NO

Preview Lets users view a list of items that were returned from a Content Search. They'll also be able to open and view each item from the list to view its contents.	NO	YES	NO	NO
Review Let's users see and open the list of the cases on the eDiscovery page in the Security & Compliance Center that they are members of. They can't perform any other case management tasks.	NO	YES	NO	YES
RMS Decrypt Let's users decrypt RMS-encrypted email messages when exporting search results or preparing search results for analysis in Advanced eDiscovery. For more information about decrypting search results during export, see Export search results from the Office 365 Security & Compliance Center.	NO	YES	NO	NO
Search And Purge Lets users perform bulk removal of data matching the criteria of a content search. For more information, see Search for and delete email messages in your Office 365 organization.	NO	NO	YES	NO

ABOUT THE AUTHOR

Daniel L. Pelc
Sr. Consultant Discovery Management

Daniel L. Pelc is a Senior Consultant for Discovery Management with NightOwl Discovery. A licensed Minnesota attorney since 1998, he advises clients on electronic discovery, litigation readiness and information governance issues. Daniel provides consulting and advisory services for global corporations with a specialty in mobility and emerging technologies. He conducts CLE programs on mobile evidence, the internet of things, and a new program on Office 365 security and implementation. Daniel received his JD from William Mitchell College of Law and his BA from the University of Minnesota.

A leader in Corporate Discovery Management, NightOwl Discovery helps companies in the most demanding industries reach their discovery, investigations and data analysis objectives. NightOwl helps enterprise customers maximize investments in people, process and technology. NightOwl provides a comprehensive and global discovery offering that spans the entire EDRM for customers in the US, EU and APAC. Please contact info@nightowldiscovery.com or visit www.nightowldiscovery.com for more information. **NightOwl Discovery - Now you're ready.**

NightOwlDiscovery®

1000 Parkers Lake Road • Wayzata, MN 55391 • 800.267.9695 • www.nightowldiscovery.com