Microsoft

Security and Compliance: Customer Controls for Information Protection in Office 365

Published: June 2014

For the latest information, please see
http://trust.office365.com

Introduction

With organizations creating and sharing an ever-increasing volume of information, the ability to protect and control data is of utmost importance. When you need visibility into what's happening or the ability to take action on your data, choosing the right application can offer immediate and immense benefits. With Office 365, we provide those tools, and give you much more. Behind these features, there are customer controls that enable you to provide the security and compliance necessity out of the gate. With software that empowers end users and compliance officers without obstructing productivity, Office 365 is here to help.

Organizations around the world trust us with the privilege of storing their most critical and important data. This privilege is never taken for granted, and we continue to innovate to provide more controls for managing the information. There are over 900 controls today, including many operating in the background in case you may need to use them in the future.

When you consider moving your organization to cloud services to store your data and various productivity services, the security, privacy and compliance concerns add another layer of consideration. Our construct for security, compliance, and privacy for Office 365 has two equally important dimensions as explained in the Office 365 Security and Compliance whitepaper. The first dimension includes service-level capabilities that include technology, operational procedures, and policies that are enabled by default for customers using the service. The second entails customer controls that include features that enable you to customize your Office 365 environment based on the specific needs of your organization. This document discusses the second dimension – customer controls that you can use to get visibility and action on your information.

We are focused on providing native tools – built from the ground up – to provide compliance and security functions to the organization. We've focused on empowering your end users to be a part of the compliance discussion and the tools to get their work done without impacting compliance. We've worked tirelessly to enable legal and compliance departments to create and respond to requests – without involvement from IT.

Overview

You may have compliance and security-related questions about the Office 365 service, the datacenter infrastructure behind it, operational issues, and if our services can help you meet your compliance objectives. Before we dig into the compliance and security features of Office 365, if you want to learn about service-level capabilities, a good place to start is the Microsoft Online Services Trust Center and the Office 365 for Enterprise Service Descriptions, which provides detailed service descriptions for all Office 365 components and includes the "Office 365 Security and Service Continuity Service Description".

Some key aspects of our customer controls for security are:

- Office 365 Message Encryption – Enables delivery of confidential business communications safely, letting users send encrypted email to any SMTP address and receive encrypted email directly from their desktops as easily as regular email
- Secure Multipurpose Internet Mail Extension (S/MIME) - Enables encryption of an email messages and allows for the originator to digitally sign the message to protect the integrity and origin of the message
- Rights Management Services – Enables a user to encrypt content using AES 128-bit keys and use policies on email or documents so that the content is appropriately used by specified people
- Role based access control – Allows administrators to enable access to authorized users based on role assignment, role authorization and permission authorization
- Transport Layer Security – Allows for server to server encryption, ensuring your email stays secure, while in motion to your partner organizations
- Exchange Online Protection - Allows administrators to manage your company's Anti-virus, Anti-spam, and anti-malware settings from within the Office 365 administration console
- Identity Management - Provides organizations with various options for identity management such as cloud based identity, identities mastered on-premises with secure token based authentication or hashed passwords to integrate into the Office 365 identity management system based on the security needs of your organization
- Multi-Factor Authentication – Enhances security in a multi-device, mobile, and cloud-centric world by using another factor, such as a PIN, in addition to the primary factor which is identity

Some key customer controls for compliance are:

- Data Loss Prevention – Helps you to identify, monitor and protect sensitive data through content analysis

- Archiving – Allows you to preserve electronically stored information retaining e-mail messages, calendar items, tasks, and other mailbox items
- eDiscovery – Permits you to retrieve content from across Exchange Online, SharePoint Online, Lync Online, and even file shares
- Auditing – Enables you to analyze logs and reports to troubleshoot configuration issues and to help you meet regulatory, compliance, and litigation requirements.

In this paper, we'll outline how Office 365 provides you the security and compliance controls you need. You'll be able to see how we have met and exceeded these needs – and how innovation continues into the future.

Information Protection Design Strategy

Built-In Tools

Recognizing the importance of an effective solution, we have delivered integrated information protection capabilities natively into Office 365. These built-in features provide a complete set of tools for the vast majority of customers without any additional installation or deployment. These security and compliance tools run the gamut – whether you need archiving, eDiscovery, data loss prevention, encryption or other security tools. All of the features were designed with an appreciation for the potential barriers that have limited wide scale adoption of bolt-on products – while working natively to help protect your organization.

We have focused on easing deployment of these features to on-premises customers, but for Office 365, the deployment step is already solved for you – with the flip of the switch, solutions like Rights Management Services or Office 365 Message Encryption are ready for use without unnecessarily complex deployments.

Empower users

With most external compliance solutions, as compliance and security policies and procedures tighten, the end user experience suffers. With Office 365, we have focused on giving you the best of both worlds – set policy to meet your business requirements and give your users powerful productivity apps that help them get their work done, wherever they are.

A great example of this thinking is with Data Loss Prevention. Many organizations have policies to prevent individuals from accidentally leaking sensitive data outside of the organization. Whether that is credit card numbers, social security numbers, a bank account number, or other sensitive data type, policy can be set to prevent or allow the transmission of this content. An administrator can even choose to allow an override behavior to allow for users to transmit the content – but in doing so acknowledge that they've understood that the content is sensitive, but need to do so anyhow in the course of business. An audit trail is started to track the sensitive transmission, but the user does not need to resort to an external service to communicate and can keep working without heavy delay.

Facilitate compliance officer independence

Legal and Compliance Officers may require visibility into organizational matters. Often times, this visibility transcends into the digital medium – a medium often managed and

maintained by IT. These requests for data can often times produce large corpus of data, be time-consuming, and tangential to the goals of the IT department. At the same time, these requests for data are often urgent and may require further action.

With Office 365, we offer a self-service solution to legal and compliance officers. Without ongoing involvement from IT, these individuals or groups can place In-Place holds, run eDiscovery queries, set up business policy preventing data loss, review audit logs, and more – all without direct involvement from IT. Office 365 also marries the principles of business policy and their technical implementation across the Office. For example, In-Place Hold or data retention will work the same way across Exchange, SharePoint or Lync data.

Security & data protection

We have implemented encryption technologies that are at the service level in Office 365. Along with this, we also offer various technologies that you can implement and configure in your Office 365 tenant. These technologies offer variety of ways to encrypt data in different workloads and offer ways to encrypt data at rest or in transit. These technologies are as follows:

- Office 365 Message Encryption
- Secure Multipurpose Internet Mail Extension (S/MIME)
- Rights Management Service
- Role-Based Access Control
- Transport Layer Security (TLS) for SMTP messages

Detailed information on these technologies can be found in Office 365 service descriptions and TechNet.

Office 365 Message Encryption

Office 365 Message Encryption delivers confidential business communications with enhanced security, allowing users to send and receive encrypted email as easily as regular email directly from their desktops. Email can be encrypted without complex hardware and software to purchase, configure, or maintain, which helps to minimize capital investment, free up IT resources, and mitigate messaging risks. Email can be sent to any email address on the Internet, including outlook.com, Yahoo! Mail, and Gmail.

Implementation of and protection of data with Office 365 Message Encryption thwarts the threats that may occur due to wire-tapping, man in the middle attack, or various forms of digital interception. This is true for email messages sent internally and externally. At the same time, any unwarranted access of email messages (in transit or at rest) is prevented via policies intrinsic to the email messages themselves. This mitigates the risk of data falling in wrong hands either knowingly or unknowingly and provides data loss prevention capabilities.

When an Exchange Online user sends an email message that matches an encryption rule, the message is sent out with an HTML attachment. A recipient opens the HTML attachment in the email message, recognizes a familiar brand if that's present, and follows the embedded instructions to sign in, open, and read the encrypted message on the Office 365 Message Encryption portal. The sign-in process helps ensure that only intended recipients can view encrypted messages.

The following diagram summarizes the passage of an email message through the encryption process.

1. An Exchange Online user sends a message to the recipient.
2. The message is filtered based on administrator-defined rules that define conditions for encryption.
3. The tenant key for your Office 365 organization is accessed and the message is encrypted.
4. The encrypted message is delivered to the recipient's Inbox.
5. The recipient opens the HTML attachment and connects to the Office 365 encryption portal.
6. The recipient authenticates using a Microsoft account or an Office 365 organizational account.
7. The tenant key for your Office 365 organization is accessed to remove encryption from the message and the user views the unencrypted message.

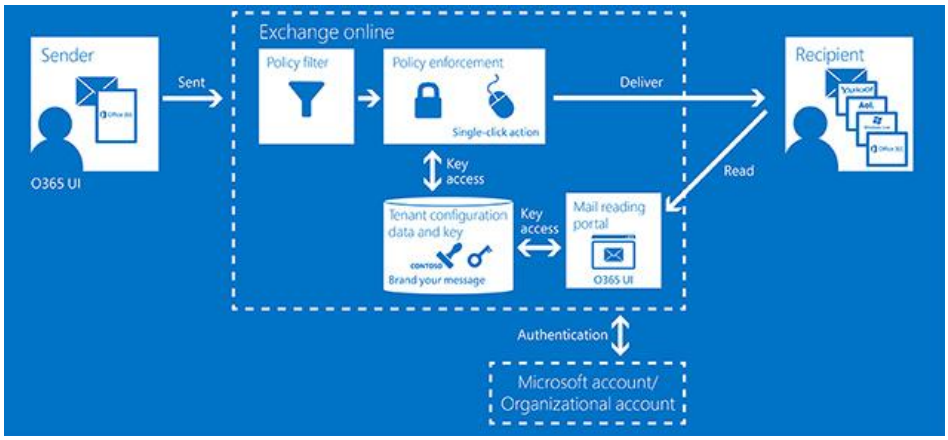


Figure 1 Office 365 Message Encryption Workflow

For more information about the keys that help ensure the safe delivery of encrypted messages to designated recipient inboxes, see Service information for Office 365 Message Encryption.

More information on OME can be found at http://msdn.microsoft.com/en-us/library/dn569286.aspx.

Secure Multipurpose Internet Mail Extension

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and digital signing of MIME data.

S/MIME allows a user to (1) encrypt an email (2) digitally sign an email. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption).

You may generate public and private certificates for end users using Public Key Infrastructure (PKI) in on-premises environment. Public certificates are distributed to your on-premises Active Directory and stored in two attributes, which can then be replicated to your tenant in Office 365.

We provide capability for end users to compose, encrypt, decrypt, read, and digitally sign emails between two users in an organization using Outlook, Outlook Web App (OWA) or Exchange ActiveSync (EAS) clients.

Figure 2 S/MIME in Outlook Web App

An email that is encrypted using S/MIME can only be decrypted by the email recipient's private certificate which is only accessible by the recipient. As such, an email message cannot be decrypted by anybody other than the recipient of the email if such an email is intercepted in transit or at rest.

You may find more information at http://technet.microsoft.com/library/dn626158.

Rights Management Services (RMS)

Rights Management Services enables end users in your organization to protect information through encryption. With RMS, end users not only encrypt data but also apply persistent usage policies such as "Do not copy", "Do not print", "Do not forward"

etc., that travel with the data to limit or allow specific actions by the recipients of the data. In addition to enabling end users to protect data and apply policies, admins can use DLP capabilities with RMS to apply RMS protection to sensitive content automatically. When combined with Data Loss Prevention, end-to-end scenarios are possible with Office 365. You can set up encryption to be performed in a Data Loss Prevention rule if sensitive content is detected. You can read the blog here to understand how to use RMS to collaborate securely.

Rights Management is also available in SharePoint to help control and protect files that are downloaded from lists or libraries. Information Rights Management encrypts the downloaded files and limits the set of users and programs that are allowed to decrypt these files. It can also limit the rights of your users who are allowed to read files, so that they cannot take actions such as print copies of the files or copy text from them.

RMS can be deployed in two forms:

- *AD RMS* - an on-premises implementation. Details can be found at http://technet.microsoft.com/en-us/library/cc771627.aspx
- *Azure RMS* - a cloud based offering of RMS with Office 365 enables easy deployment of RMS. Azure RMS can be deployed for an entire organization with a few clicks in a matter of seconds. Details on Azure RMS can be found at http://technet.microsoft.com/en-us/library/jj585016.aspx. With the default implementation, where encryption keys are generated and managed by Office 365, content is encrypted using AES 128 bit key and each content key is encrypted with RSA 2048 bitkey.

With the protection of data using Azure RMS, you can defend against threats that may occur due to wire-tapping, man in the middle attack etc.,

Role-based Access Control

Role-Based Access Control (RBAC) is a principle that is implemented across Office 365 at the service-level and in customer controls. At the service-level, the design principles for administrative access are outlined in the Office 365 Security whitepaper.

As a customer control, RBAC is implemented at the Office 365 admin level and also at more granular levels.

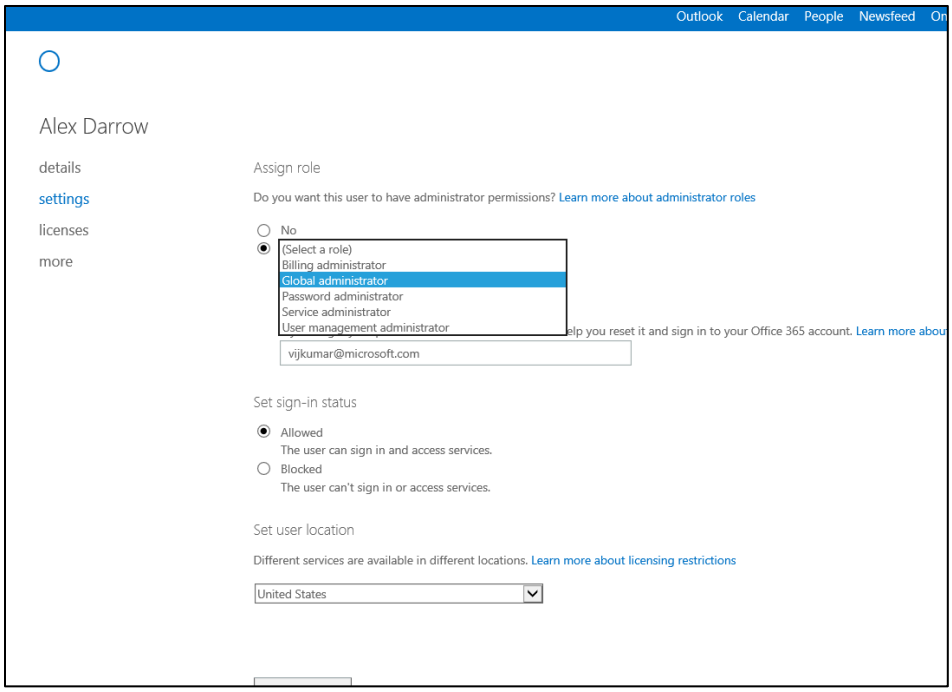
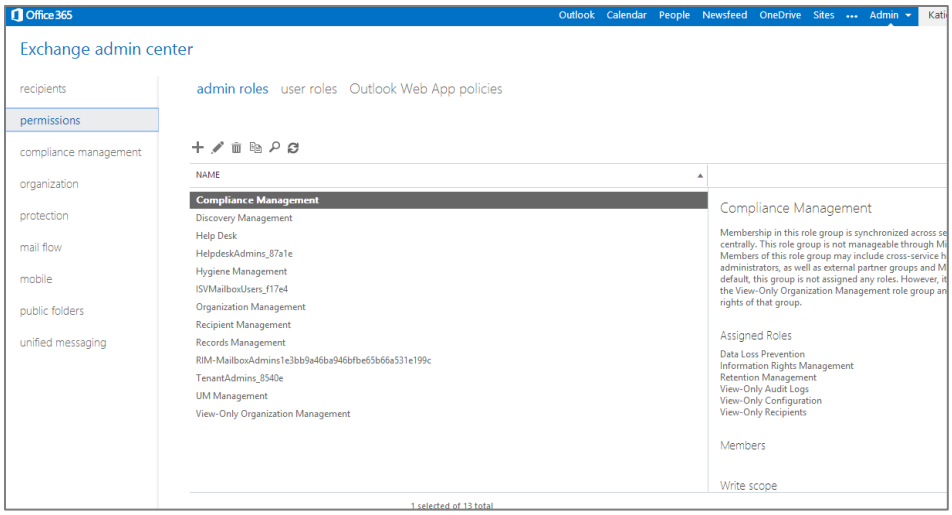


Figure 3 Example of further granular RBAC in Office 365

Role-Based Access Control (RBAC) is a mechanism for restricting access to resources based on a person's or group's role. RBAC also enables you to more closely align the roles you assign users and administrators to the actual roles they hold within your organization. In Office 365, RBAC controls both the administrative tasks that can be performed and the extent to which users can now administer their own services. An Office 365 administrator can also enable and disable certain roles to further modify control what properties and/or features a user can manage.

A summary of the administration of built-in roles can be found at http://technet.microsoft.com/en-us/library/hh852528.aspx.

Similarly there is RBAC for Compliance Management



Transport Layer Security for SMTP messages

You may setup an SMTP connection to trusted partners that is secured using Transport Layer Security negotiation. The connector can be set to send emails using either opportunistic or forced TLS.

Sending email via an encrypted SMTP channel can prevent data in emails from being stolen in man in the middle attack where your organizations is sending or receiving emails to a business partner.

More information can be found at http://technet.microsoft.com/en-us/library/exchange-online-mail-flow.aspx.

Exchange Online Protection

Exchange Online Protection (EOP) is the cloud email filtering service that protects against malware, viruses and spam. Available within the Office 365 Admin center, EOP makes use of geographically balanced data centers, queuing mail capabilities to give you an enterprise-class reliability and protection against spam and malware, while maintaining access to email during and after emergencies.

EOP provides a multi layered spam protection that includes connection filtering, that blocks up to 80% of all spam based on IP block/allow list, Sender-recipient filtering that blocks up to 15% of all spam based on internal lists and sender reputation, and content filtering that blocks 5% of all spam based on internal lists and heuristics.

Microsoft

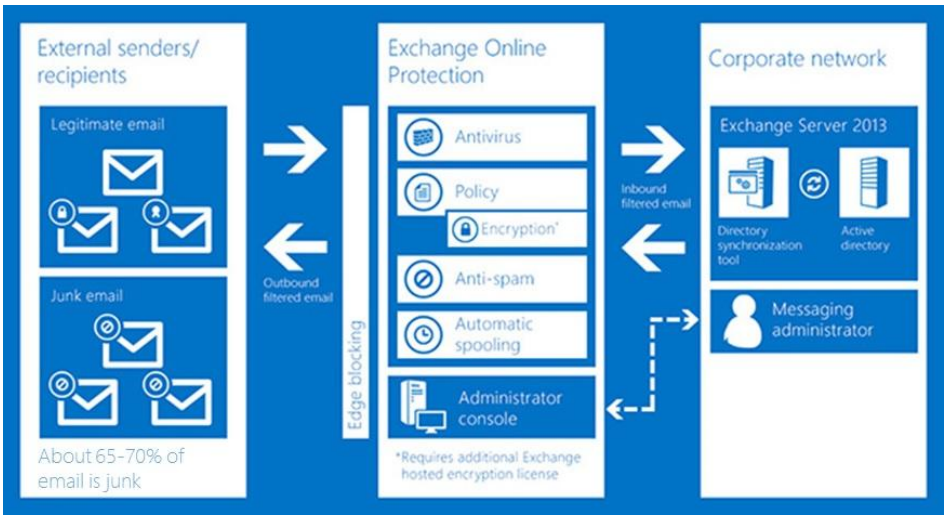


Figure 4 Exchange Online Protection Controls and Workflow

EOP provides a granular anti-spam filtering controls making use of connection filtering, multiple content spam categories such as obvious spam and high confidence spam and new content filtering actions. Organizations can take specific actions for the bulk messages and also block emails based on language and geography. Your users can also use the enhanced Junk Email Reporting Add-in for Outlook in order to report junk (spam) messages to us for analysis.

Your administrators can also configure rules on how to manage junk mail. Your user's safe senders and block lists are automatically synchronized with the EOP service. Administrators and end users have the capability to access quarantine and release messages. In addition, end user spam notifications are available for the users to review the messages and take necessary action.

EOP rules are built on top of Exchange Transport Rules (ETR's) which are based on a simple and easy to use predicate of conditions, actions and exceptions. EOP also includes built in reporting options for your organizations and a downloadable excel workbook to further analyze data.

EOP runs on a worldwide network of Office 365 data centers that are designed to provide the best availability. We currently operate data centers in various regions such as North America and EMEA, including a Government Community Cloud in the U.S. We maintain and guarantee geocentric affinity in these two regions, meaning that the data sent within a region is processed within that region. We're expanding geocentric affinity for EOP to the Asia-Pacific (APAC) region. Currently, all Exchange Online mailboxes for APAC customers are already located in APAC data centers, and later this year messages will be routed through APAC data centers for EOP filtering.

More information can be found at:
http://technet.microsoft.com/library/jj723119(v=exchg.150).aspx

Identity Management

Your company directory is the list of users who can sign in to use applications and the users that you can look up so you can send an email or grant access to documents. We provide three ways for you to manage user accounts in your directory:

- No on-premises deployment (Cloud Identities without Directory Synchronization)
- Directory and Password Synchronization
- Federated Identities (with Directory Synchronization)

Cloud identity is when you choose to store your identity information in Office 365 – without any on-premises directory synchronization. In this scenario, Identity Services is used to establish, manage, and authenticate your users. User accounts are cloud-managed by using a web portal and Azure Active Directory in Office 365. No servers are required.

With Directory and Password Synchronization, on-premises directory objects (users, groups, contacts) are automatically synchronized to the Office 365 directory, reducing administrative overhead. As part of the Directory Synchronization process, your end user passwords (hashes) can also be synchronized as well, enabling your users to sign in to Office 365 services using the same name and password as they use to log onto corporate network and resources. This experience is known as "same sign-on" and users may experience more password prompts than federated customers. However, because passwords can be cached and remembered on the client, in practice the amount of prompting can be minimized to acceptable levels.

The final option if you have an on-premises directory and authentication infrastructure is to implement federation with Office 365. For this, a compatible Secure Token Service infrastructure such as Active Directory Federation Services is required. Once enabled, your users can use their Active Directory corporate credentials (user name and password) to access the services in the cloud and their existing on-premises resources, in a seamless manner. When using federation, every authentication request against Office 365 is validated against the on-premises authentication infrastructure. Federation also allows customers to implement additional features, such as client access policies, integration with two-factor authentication services or logon auditing. If you need to integrate Office 365 with an existing (third-party) identity provider that holds your directory, please review the *Works with Office 365-Identity* program, which is described here: http://blogs.office.com/2013/09/03/works-with-office-365-identity-program/

Multi-Factor Authentication

Multi-factor authentication enhances security in a multi-device and cloud-centric world. We provide a built-in solution with Office 365 for multi-factor authentication through a phone call, text message, or notification on a dedicated app. We also support third-party multi-factor authentication solutions.

Built-in multi-factor authentication options include:

- Notify me through app. The user configured a smartphone app and they receive a notification in the app that they must confirm the login. Smartphone apps are available for Windows Phone, iPhone, and Android devices.
- Show one-time code in app. The same smartphone app is used. Instead of receiving a notification, the user starts the app and enters the six-digit code from the app into the portal.
- Text code to my mobile phone. The user receives a text message containing a six-digit code that they must enter into the portal.
- Call my mobile phone. The user receives a phone call that asks them to press the pound key. Once the pound key is pressed, the user is logged in.
- Call my office phone. This is the same as Call my mobile phone, but it enables the user to select a different phone if they do not have their mobile phone with them.

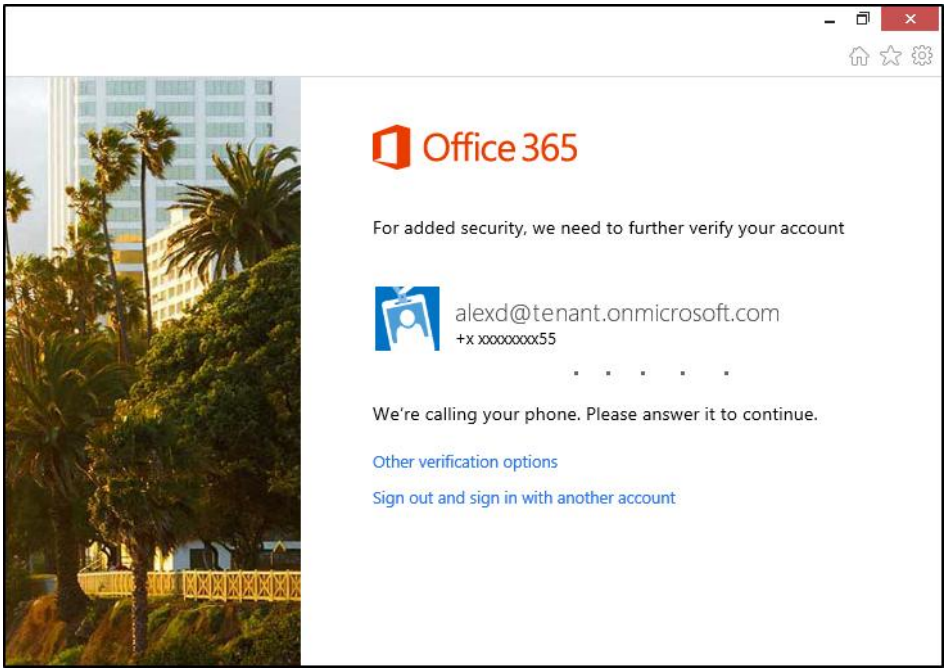


Figure 5 Multi-factor authentication calling phone

Your users that are enrolled into multi-factor authentication will be required to configure App Passwords in order to use Office desktop applications, including Outlook, Lync, Word, Excel, PowerPoint, and OneDrive for Business.

Once a user has logged in with multi-factor authentication, they will be able to create one or more App Passwords for use in Office client applications. An App Password is a 16-character randomly generated password that can be used with an Office client application as a way to increase security in lieu of the second authentication factor.

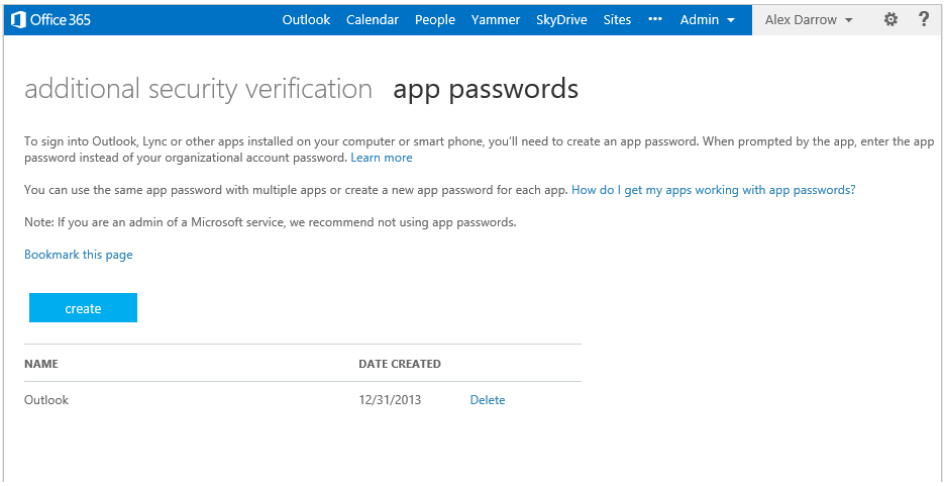


Figure 6 App Password for an Office desktop application in your account

For more information about Multi-Factor Authentication for Office 365 please read the TechNet article [Multi-Factor Authentication for Office 365]

Microsoft

Compliance

With Office 365, you not only get the benefit of compliance with standards and regulations, you also get compliance controls that allow visibility and control into your data.

You get visibility into your data, ability to see who has accessed it and the ability to take actions on it such as proactively protect it, preserve it or for that matter delete it entirely. All these compliance controls are within Office 365.

Data Loss Prevention

Data loss prevention in in Office 365 helps you identify, monitor, and protect sensitive information in your organization through deep content analysis. DLP is increasingly important for enterprise message systems, because business-critical email often includes sensitive data that needs to be protected. Worrying about whether financial information, personally identifiable information (PII), or intellectual property data might be accidently sent to unauthorized users can keep a Chief Security Officer (CSO) up all night. Now you can protect sensitive data more easily than ever before, without affecting worker productivity.

With DLP Policy Tips in Office 365, administrators can inform email senders that they may be about to pass along sensitive information that is detected by the company's policies - before they click Send. This helps your organization stay compliant and it educates your employees about custom scenarios based on your organization's requirements. It accomplishes this by emphasizing in-context policy evaluation. Policy Tips not only analyze email messages for sensitive content, but also determine whether information is sensitive in the context of communication. That means you can target specific scenarios that you associate with risk, external communication for example, and configure custom policy tips for those scenarios. Reading those custom policy tips in email messages keeps your workers aware of your organization's compliance policies and empowers them to act on them, without interrupting their work.

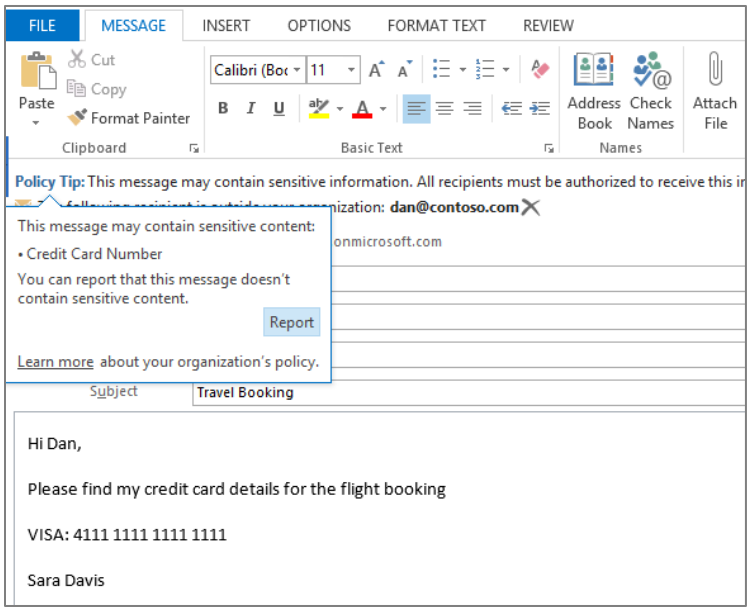


Figure 7 DLP Policy Tip showing sensitive content

You can configure policy tips that will merely warn your users, block their messages, or even allow them to override your block with a justification. At the same time, you have the ability to track and monitor any of these actions.

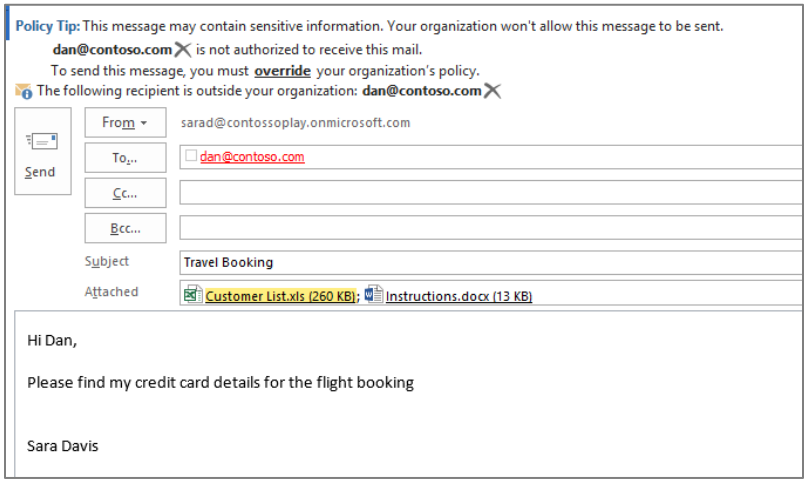


Figure 8 DLP Policy Tip highlighting attachment

Data loss prevention empowers end users, making them part of the organization's compliance process and ensuring that the business flow is not interrupted or delayed, because achieving compliance does not get in users' way. At the same time, data loss

prevention simplifies compliance management for admins, because it enables them to maintain control in the Office 365 admin portal.

Policy Tips are similar to MailTips, and can be configured to present a brief note to provide information about your business policies to the person crafting the email message. Policy Tips can merely warn workers, block their messages, or even allow them to override your block with a justification. Policy Tips can also be useful for fine-tuning DLP policy effectiveness, as end users easily report false positives.

Additionally, you may encounter scenarios in which individuals in your organization email many kinds of sensitive information during a typical day. Document Fingerprinting makes it easier for you to protect this information by identifying standard forms that are used throughout your organization and allowing you to take action on the communication.

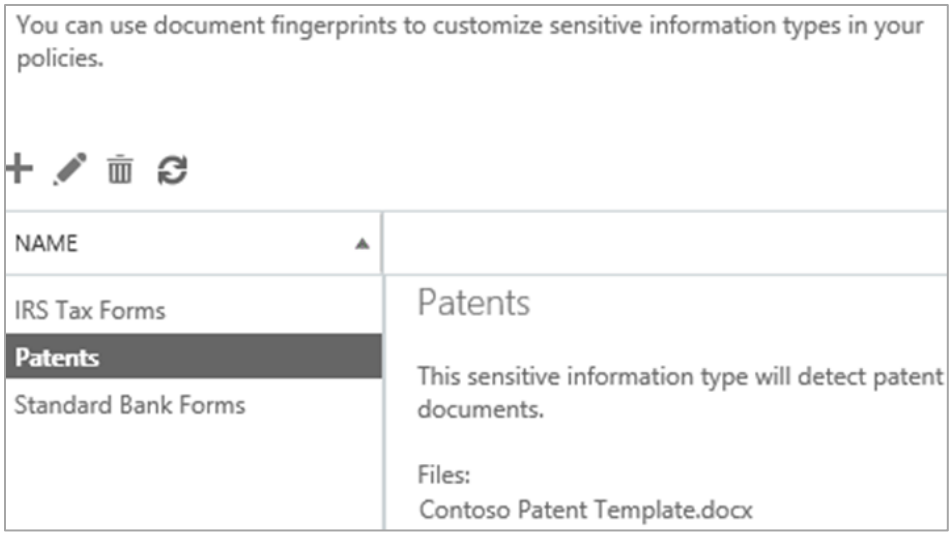


Figure 9 DLP Document Fingerprinting

Incident reports are also triggered when an action occurs. Such incident reports can help you track events in real time, because a report is generated in real time and sent to a designated mailbox, such as the mailbox for incident manager account.

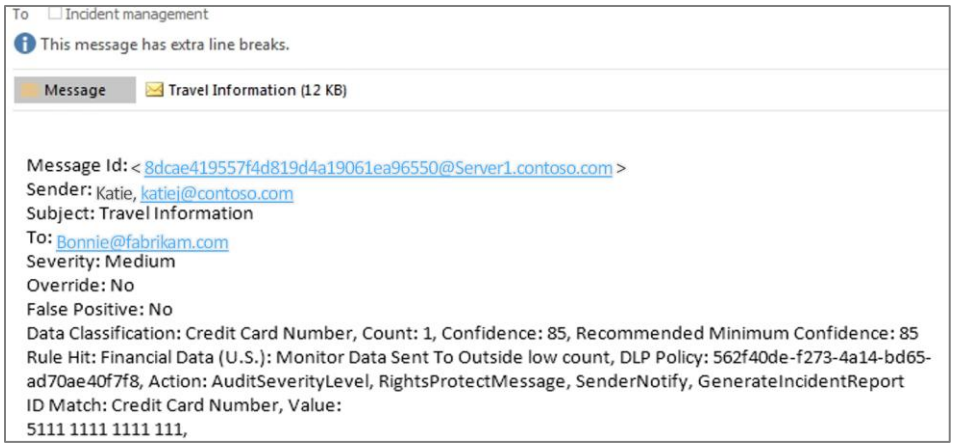


Figure 10 Incident Report

In addition to enabling end users to protect data and apply policies, admins can use DLP capabilities with Rights Management Services and/or Office 365 Message Encryption to further encrypt and protect sensitive content automatically. For more information please see: http://technet.microsoft.com/en-us/library/exchange-online-service-description.aspx

Email Archiving

Whether tracking down an old message or running an eDiscovery request to find information, the preservation of email is critical for businesses. Ever-increasing volumes of email stress users' ability to organize and manage their inbox, while IT is challenged with protecting and maintaining that information. With Office 365, large mailboxes and archiving with unlimited storage space are built into the email platform. Users can have the full functionality that they expect with Outlook and Exchange, while compliance officers can rest at night knowing their legal and data retention needs are being met.

Your users can access archived and current email quickly and easily, and they no longer have to waste time managing their inboxes to stay within quotas. They also do not need to store messages in .PST files outside the control of Exchange administrators and backup policies. Finally, all of their mailbox folder hierarchy stays exactly in-place, without any modification.

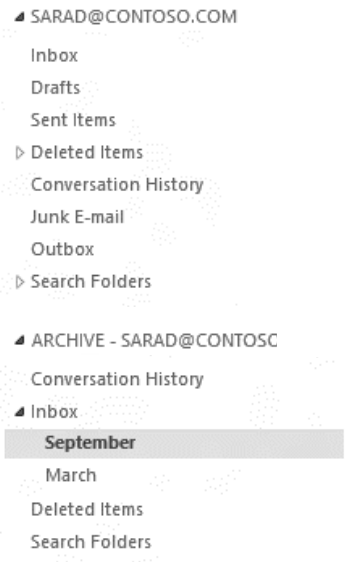


Figure 11 Folder hierarchy of In-Place Archive

From the perspective of IT, administrators have the flexibility to balance storage performance and cost to suit business needs. They can manage and search archived and current email through one interface and no longer need to deploy and maintain separate archiving infrastructure. This also means they have a single place to manage compliance and retention.

Data Retention and Lifecycle

For business, legal, or regulatory reasons, you may have to retain e-mail messages sent to and from users in your organization, or you may want to remove e-mail that you aren't required to retain. Messaging records management (MRM), the records management technology in Office 365, enables you to control how long to keep items in users' Exchange mailboxes and SharePoint documents and define what action to take on items that have reached a certain age.

MRM in Exchange Online is accomplished by using *retention tags* and *retention policies*. An overall MRM strategy is based on:

- Assigning *retention policy tags* (RPTs) to default folders, such as the Inbox and Deleted Items.
- Applying *default policy tags* (DPTs) to mailboxes to manage the retention of all untagged items.
- Allowing the user to assign *personal tags* to custom folders and individual items.

- Separating MRM functionality from users' Inbox management and filing habits. Users aren't required to file messages in managed folders based on retention requirements. Individual messages can have a different retention tag than the one applied to the folder in which they're located.

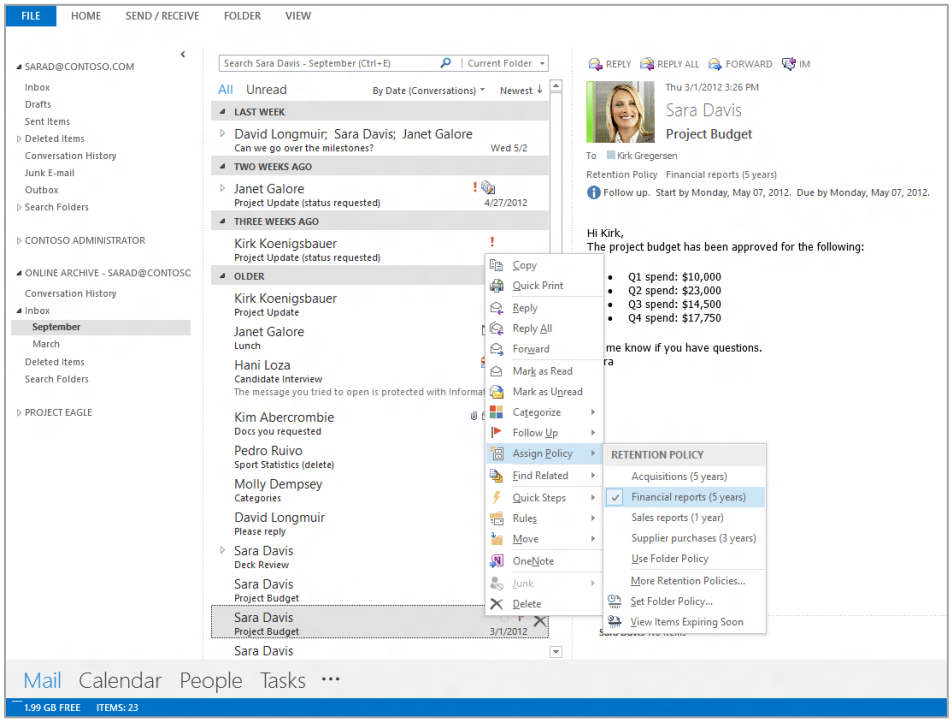


Figure 12 End user choosing retention policy

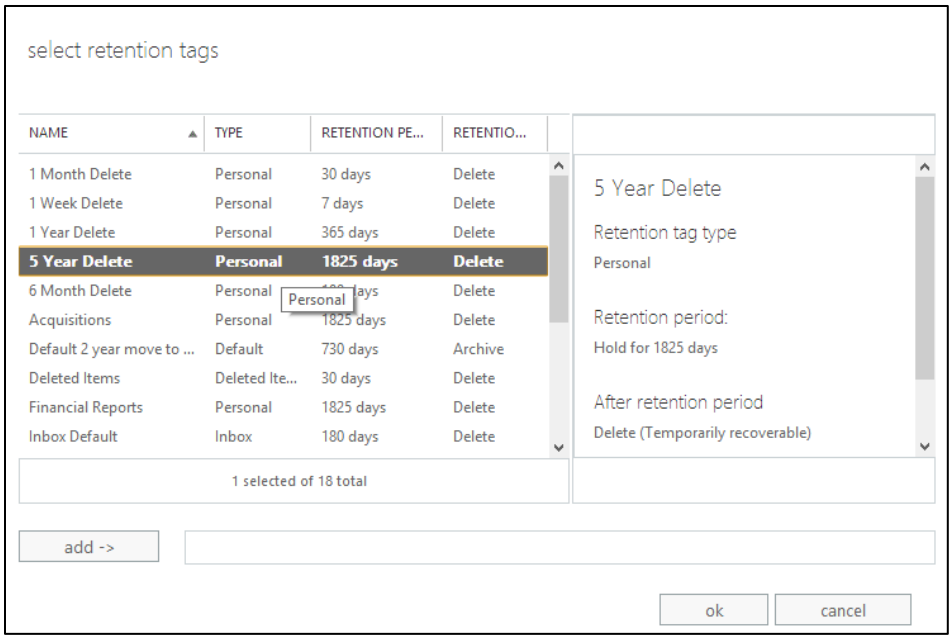


Figure 13 Exchange Policy

SharePoint Online also uses policy driven behavior to retain, audit, or delete documents after a specified period of time. Document deletion policies can be assigned to site templates or even individual site collections. With a document deletion policy, you can proactively reduce risk by deleting documents in a site after a specific period of time — for example, you can delete documents in users' OneDrive for Business sites five years after the documents were created. Information management policies can be assigned to a Content Type or Library and can specify how long a type of content should be retained and what should be audited. This policy feature lets you define retention stages, with an action that happens at the end of each stage. For example, you could define a two-stage retention policy on all documents in a specific library that deletes all previous versions of the document one year after the document is created, and declares the document to be a record five years after the document is created.

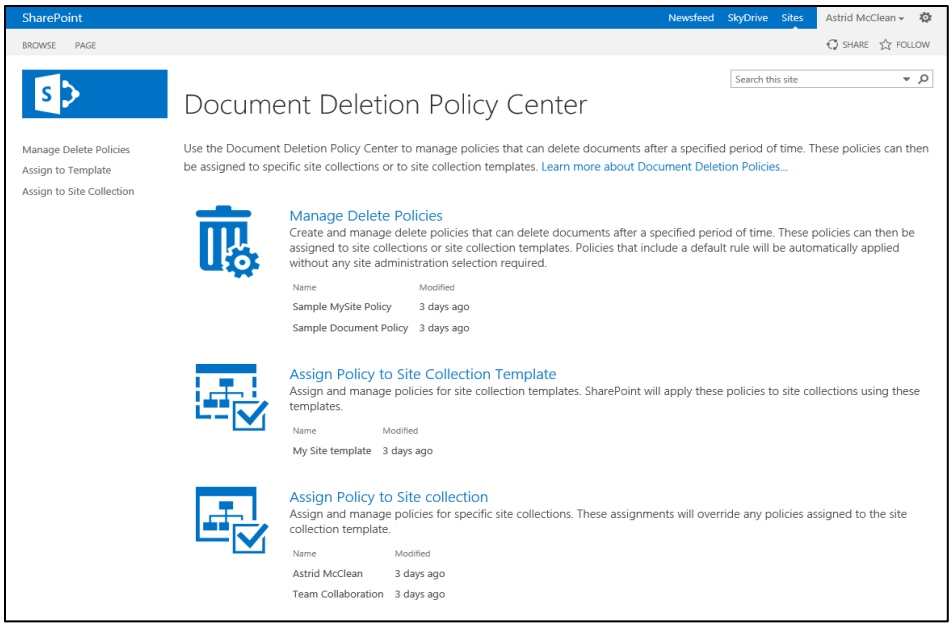


Figure 14 SharePoint Document Deletion Policy Center

eDiscovery

Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence. Office 365 includes the eDiscovery Center, which serves as a portal for managing eDiscovery cases. From this central place you can discover content in SharePoint, Exchange, and Lync.

When you receive a new request for eDiscovery, you can create an *eDiscovery case* in the eDiscovery Center – without continuing to involve IT. An eDiscovery case is a collaboration site that you can use to organize information related to the eDiscovery request.

The two primary components of an eDiscovery case are *eDiscovery sets* and *queries*. Use an eDiscovery set to find content and apply a hold. Use a query to find content and export it.

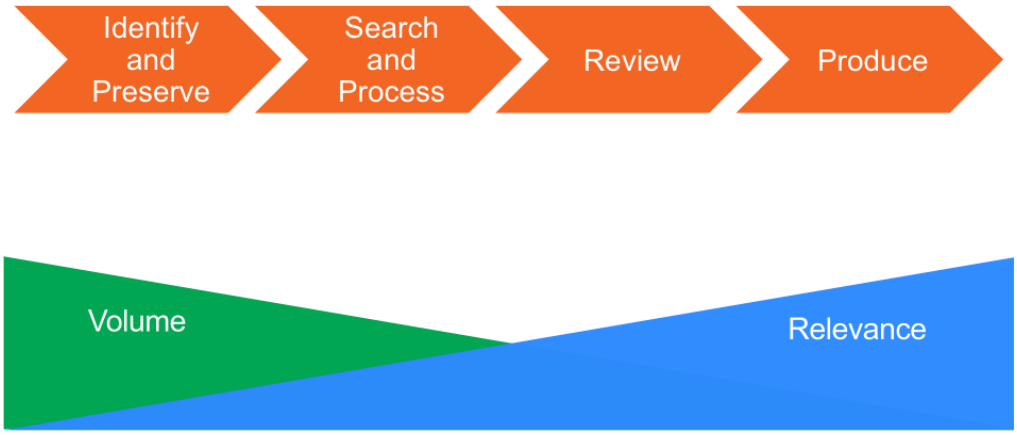


Figure 15 eDiscovery Process Flow

eDiscovery Center also allows you to place an In-Place Hold. When an in-place hold is set, the content in an Exchange mailboxes, Lync Instant message and meeting content, SharePoint sites, or OneDrive for Business files remain in its original location. Your users can still work with and modify the content, but a copy of the content as it was at the time that you initiated the hold is preserved. Additionally, if an In-Place Hold is applied to the content, any new content that is created or added to the mailbox or site will be discoverable, and will be preserved even if deleted by the user.

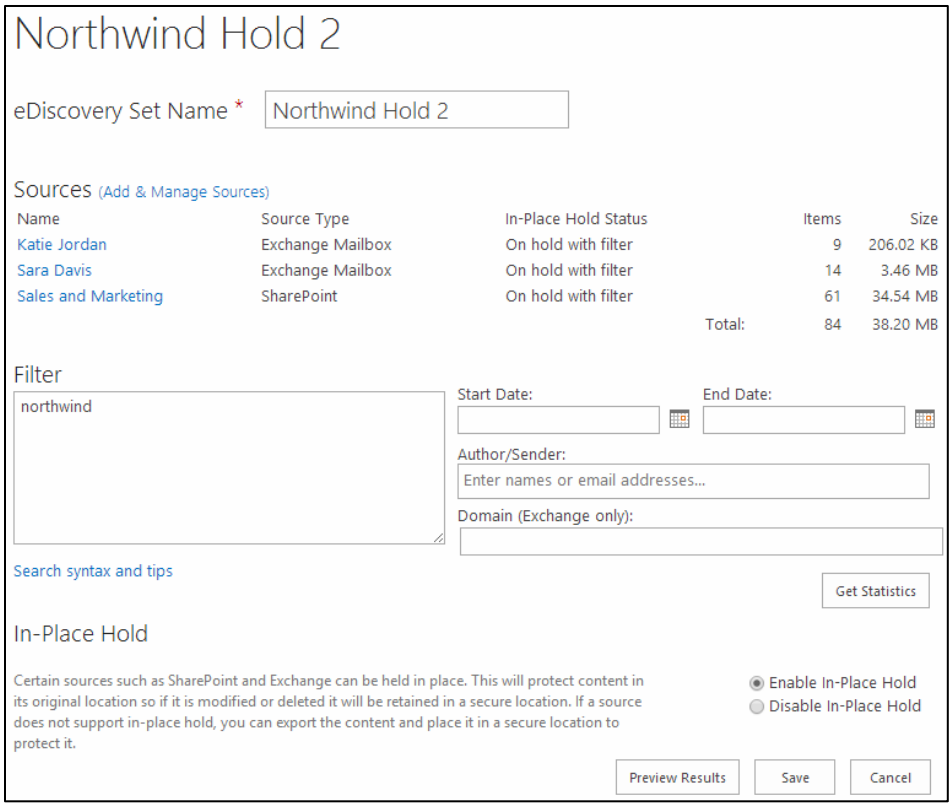


Figure 16 Query and Hold

When you have identified the specific items that you will have to deliver, you can export them in an industry-standard EDRM (Electronic Discovery Reference Model) format.

Auditing

Use audit logging and reporting to troubleshoot configuration issues by tracking specific changes made by administrators and to help you meet regulatory, compliance, and litigation requirements. Office 365 provides the following audit reports:

- **Non-Owner Mailbox Access Report (Exchange)** - Reports mailboxes that have been accessed by someone other than the person who owns the mailbox.
- **In-Place Hold Report (Exchange)** - Reports mailboxes that were put on or removed from hold
- **Administrator Role Group Report (Exchange) -** Reports changes made to administrator role groups

- **Content modifications (SharePoint)** - Reports changes to content, such as modifying, deleting, and checking documents in and out.
- **Content type and list modifications (SharePoint)** - Reports additions, edits, and deletions to content types.
- **Content viewing (SharePoint)** - Reports users who have viewed content on a site.
- **Deletion (SharePoint)** - Reports what content has been deleted.
- **Run a custom report (SharePoint)** - You can specify the filters for a custom report, such as limiting the report to a specific set of events, to items in a particular list, to a particular date range, or to events performed by particular users.
- **Expiration and Disposition (SharePoint)** - Reports all events related to how content is removed when it expires.
- **Policy modifications (SharePoint)** - Reports on events that change the information management policies on the site collection.
- **Auditing settings (SharePoint)** - Reports changes to the auditing settings.
- **Security settings (SharePoint)** - Reports changes to security settings, such as user/group events, and role and rights events.

Furthermore, audit reports are available for actions administrators have performed. We also obtain third-party audits and certifications so you can trust our services are designed and operated with stringent safeguards.

- **Office 365 –** Reports portal creation of users and all password resets. Available through Office 365 technical support
- **Exchange Online –** Reports Exchange mailbox access. Available from Exchange Control Panel
- **SharePoint Online –** Reports SharePoint site and storage access. Available from Office 365 technical support
- **Datacenter audit reports:** For more detail on all third party audits, please see: http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm

Conclusion

With Office 365, your organization can finally use the productivity tools they want to be successful, while ensuring you have visibility and control over everything surrounding the information.

The data you store in Office 365 is fully protected with built-in tools to help you manage it in-place. There is no longer a need to manage a variety of tools to archive, search, prevent the loss of sensitive information, or encrypt your data. With Office 365, archiving, eDiscovery, data loss prevention, and encryption are all built into the service and ready to use without complicated deployments.

Users can delight in the fact that they can use the Office clients and apps they use every day. They don't need to waste time learning new tools or complicated processes to get their work done, wherever they are. And you can feel comfortable knowing that your compliance and security policies are met.

With Office 365, you can manage your workflow without direct involvement from IT. This finally allows you to have a clear separation of boundaries between the divisions in the organization. With Office 365, you can get your work done, have visibility and control over the data and help your users be more productive in their daily jobs.

To learn more about this and other security and compliance topics with Office 365, please visit http://trust.office365.com.

Microsoft