American
Technology Services
a WWTS Company

Securing Office 365 *for free*

Office 365 Threat Landscape

How are the bad guys attacking you?

Threat Landscape

Attackers are focusing on people, not technology

- Password spraying
- Brute force login attempts
- Phishing/Social Engineering
- Misconfigured services

Protecting Identities

Because you can’t install antivirus on your users.

Multifactor Authentication

Yes, it's that important.

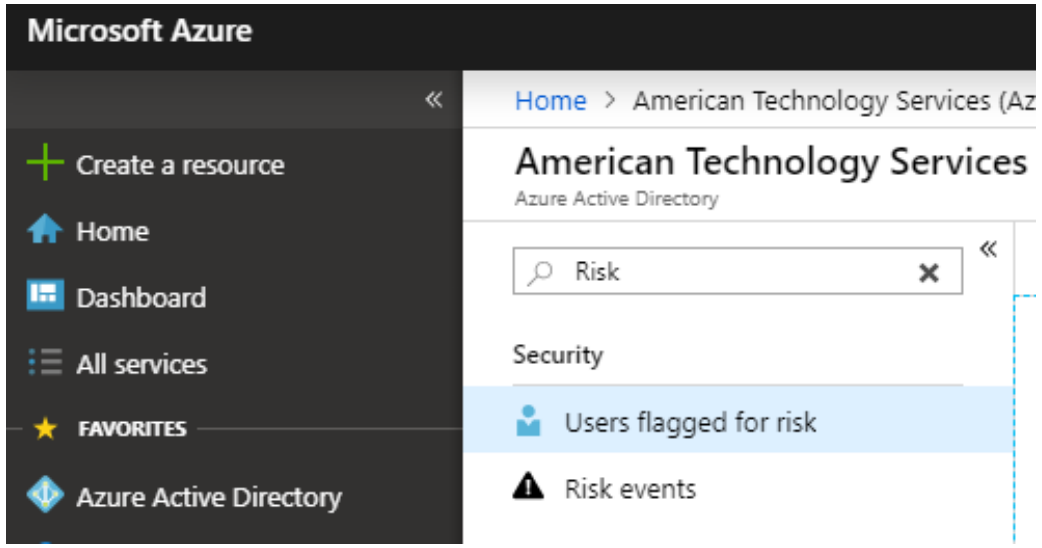
Available Methods:

- Random code
- Push notification
- Phone call/Text
- Smart card
- Biometric device

Available to all license levels. Azure AD Premium unlocks advanced features.

Risky sign-in report

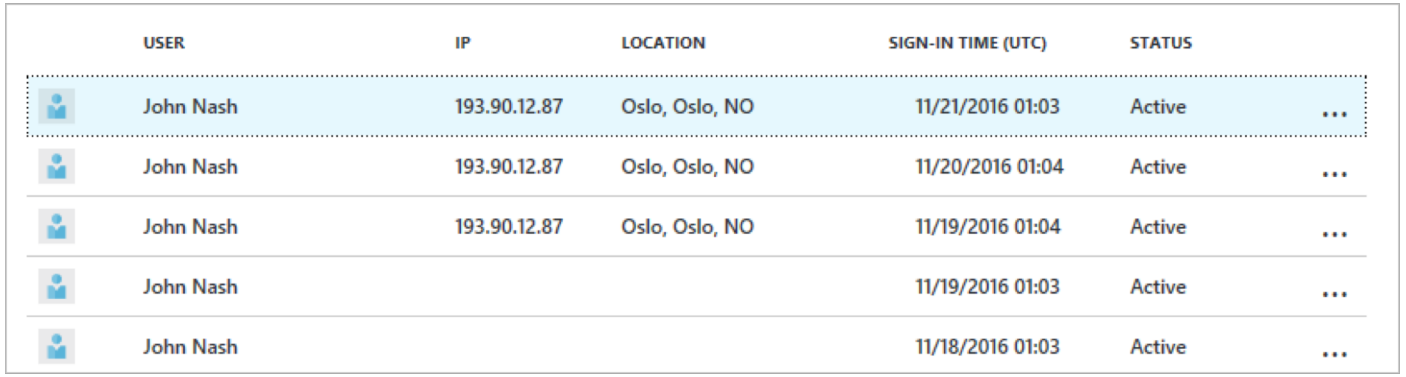
Why did Sara log in from Virginia this morning and Nigeria tonight?



Available to all license levels. Azure AD Premium unlocks advanced features.

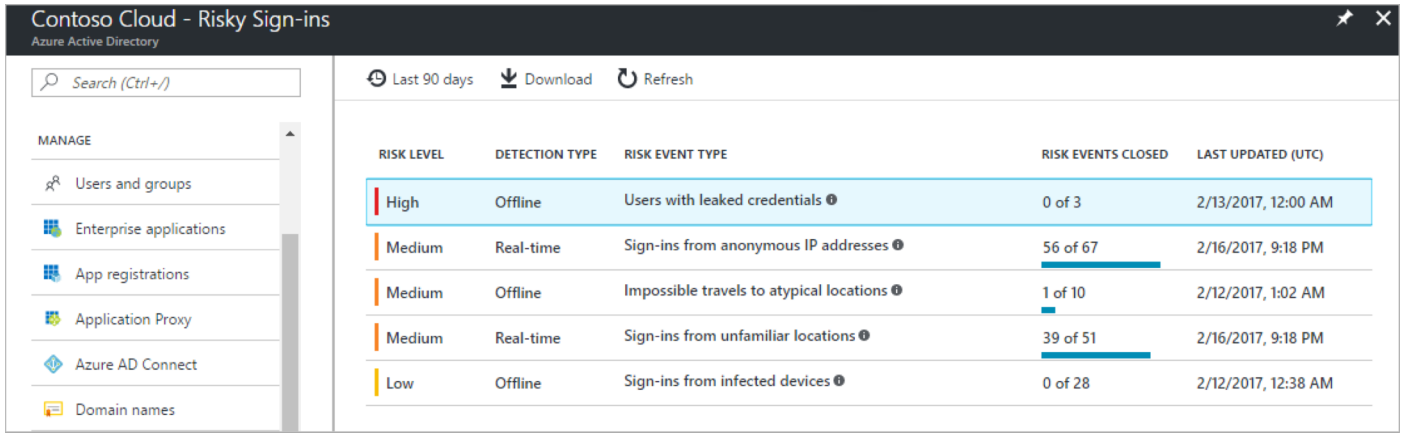
License Level Comparison

Free and Basic Editions



USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
John Nash	193.90.12.87	Oslo, Oslo, NO	11/21/2016 01:03	Active
John Nash	193.90.12.87	Oslo, Oslo, NO	11/20/2016 01:04	Active
John Nash	193.90.12.87	Oslo, Oslo, NO	11/19/2016 01:04	Active
John Nash			11/19/2016 01:03	Active
John Nash			11/18/2016 01:03	Active

Azure AD Premium



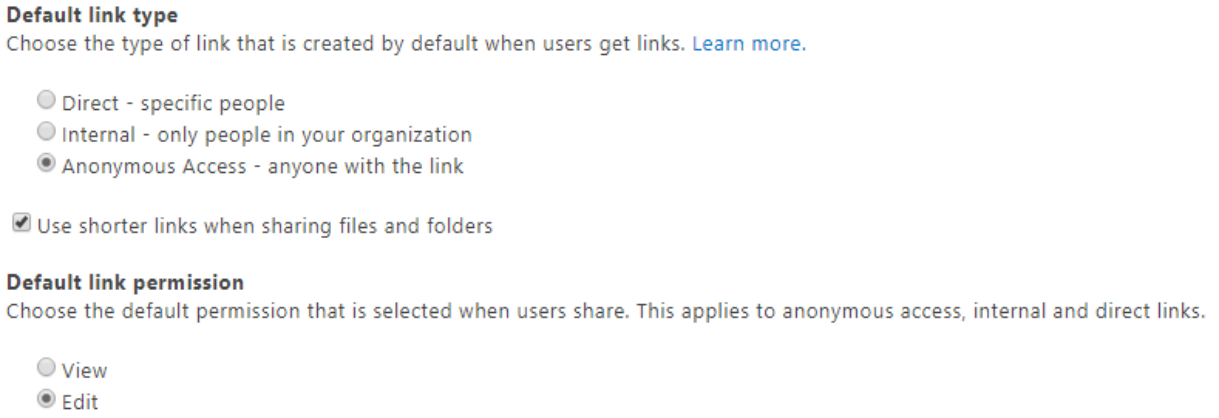
Protecting Data

Are users giving away your sensitive documents?

Default SharePoint permissions

Oh yea, I forgot about that.

Available Methods:



Available to all license levels.

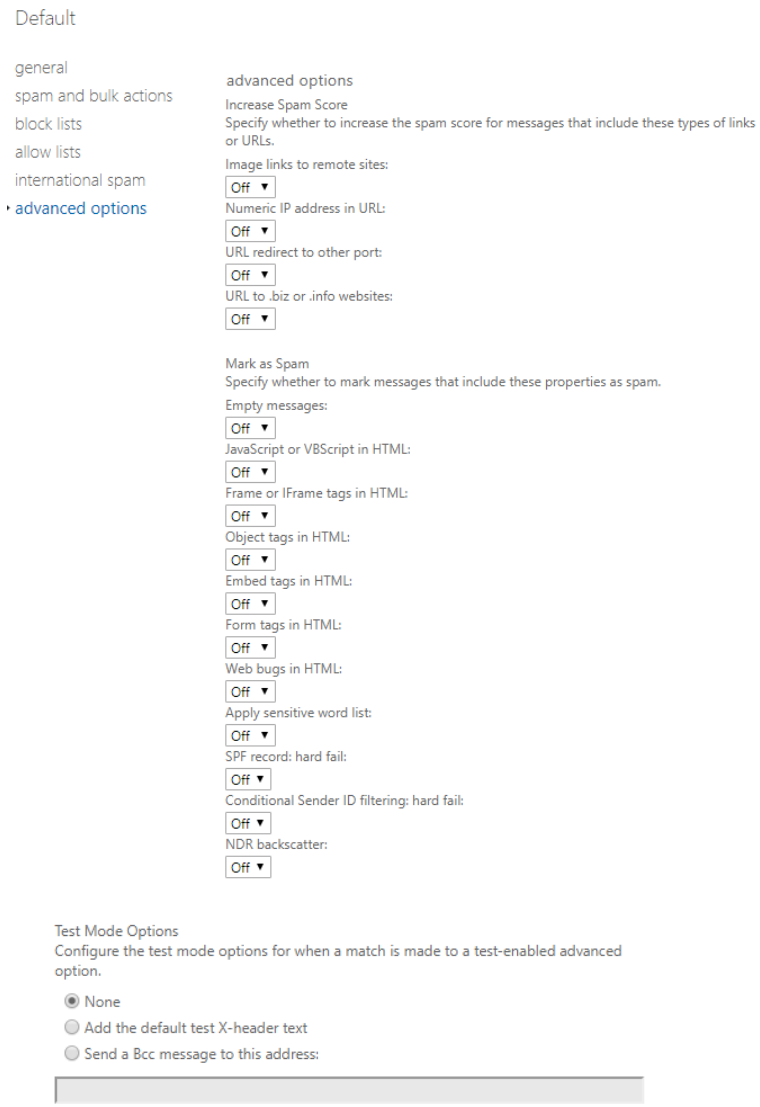
Protecting Email

Where does all this spam come from, anyway?

Tweaking the spam filter

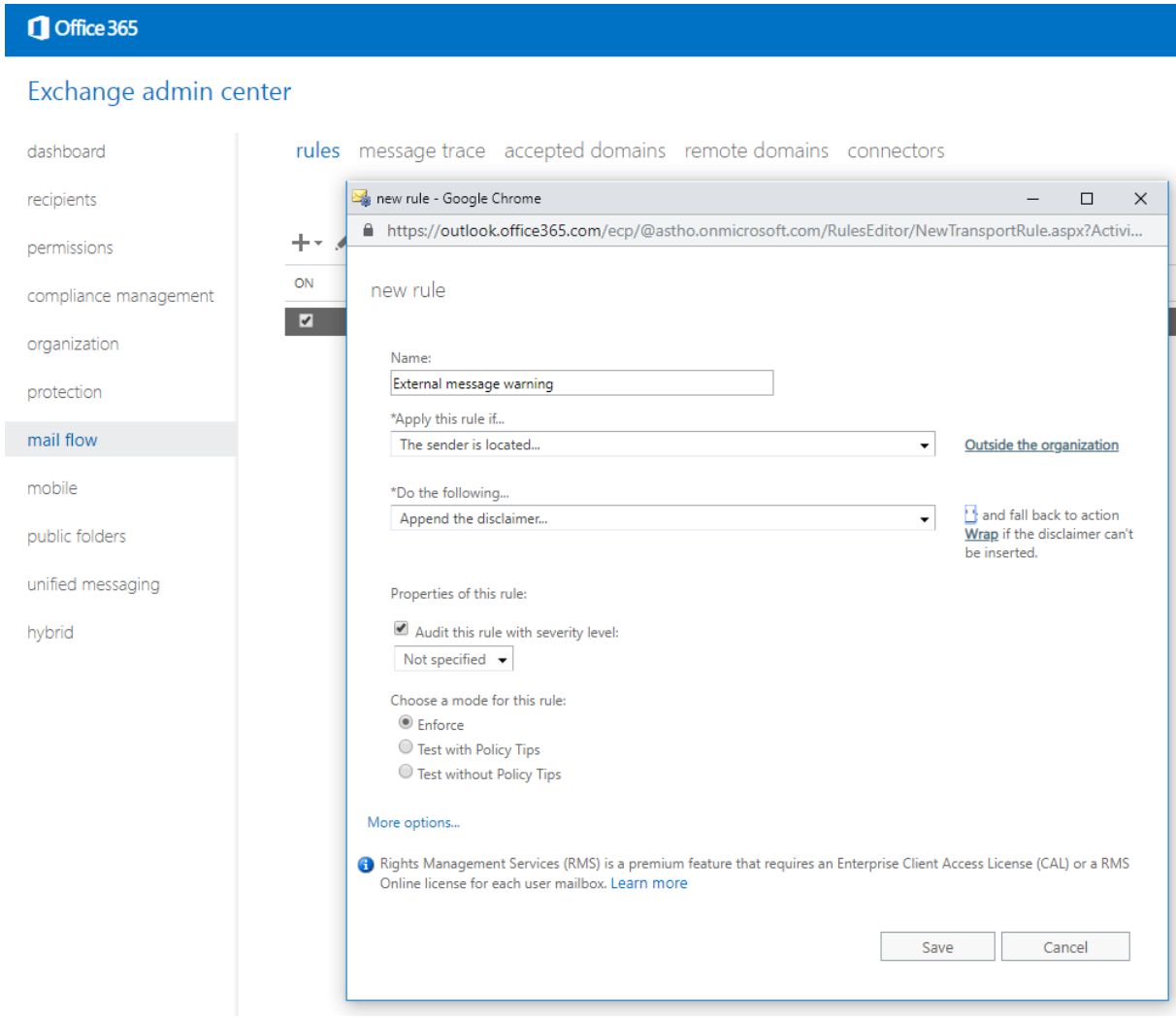
A tragically unused option.

Available Options:



Available to all license levels.

External email banner



Available to all license levels.

“Advanced” DNS config

SPF, DKIM and DMARC, oh my!

- SPF – *Tells the world where your email should come from.*
- DKIM – *Cryptographically sign each email to prove it came from you.*
- DMARC – *Additional checks to identify incoming spoofed emails.*

Available to all license levels.

Mailbox audit logging

Tracing the bad guys' steps.

Why auditing?

Enabled by default…sort of.

Get-OrganizationConfig | FL AuditDisabled

(Exchange Online Powershell)

What is audited?

Available to all license levels.

Mailbox audit logging

Continued

Default settings:

Action	Description	Admin	Delegate	Owner
Copy	A message was copied to another folder.	Yes	No	No
Create	An item is created in the Calendar, Contacts, Notes, or Tasks folder in the mailbox; for example, a new meeting request is created. Note that creating, sending, or receiving a message isn't audited. Also, creating a mailbox folder is not audited.	Yes*	Yes*	Yes
FolderBind**	A mailbox folder was accessed. This action is also logged when the admin or delegate opens the mailbox.	Yes	Yes	No
HardDelete	A message was purged from the Recoverable Items folder.	Yes*	Yes*	Yes*
MailboxLogin	The user signed into their mailbox.	No	No	Yes
MessageBind***	A message was viewed in the preview pane or opened.	Yes	No	No
Move	A message was moved to another folder.	Yes	Yes	Yes
MoveToDeletedItems	A message was deleted and moved to the Deleted Items folder.	Yes*	Yes*	Yes*
SendAs	A message was sent using the SendAs permission. This means another user sent the message as though it came from the mailbox owner.	Yes*	Yes*	No
SendOnBehalf	A message was sent using the SendOnBehalf permission. This means another user sent the message on behalf of the mailbox owner. The message indicates to the recipient who the message was sent on behalf of and who actually sent the message.	Yes*	Yes*	No
SoftDelete	A message was permanently deleted or deleted from the Deleted Items folder. Soft-deleted items are moved to the Recoverable Items folder.	Yes*	Yes*	Yes*
Update	A message or its properties was changed.	Yes*	Yes*	Yes*

On your way to greener pastures. Questions?

American Technology Services
a WWTS Company

Thank You

Chris Schoenwetter

(703) 876-0300

cschoenwetter@networkats.com

networkats.com