



When Worlds Collide: Security in a Cloud-Enabled Environment

Sean Metcalf, CTO
Trimarc



Presenter bio



Sean Metcalf

- Trimarc Founder (help companies better secure their Microsoft platform)
- One of ~100 people globally who holds the Microsoft Certified Master Directory Services (MCM) certification.
- Presented on Active Directory attack and defense at Black Hat, BlueHat, BSides, DEF CON, DerbyCon, Shakacon and Sp4rkCon security conferences.
- Post info on [ADSecurity.org](https://adsecurity.org)



Agenda

- The “Cloud”
- Cloud Security Challenges
- Identity Management in the Cloud (Active Directory)
- Exploit Scenarios
- Office 365 Auditing & Logging
- Microsoft Cloud Security: What Really Matters
- Recommendations & Wrap-up









On-Premises vs Cloud

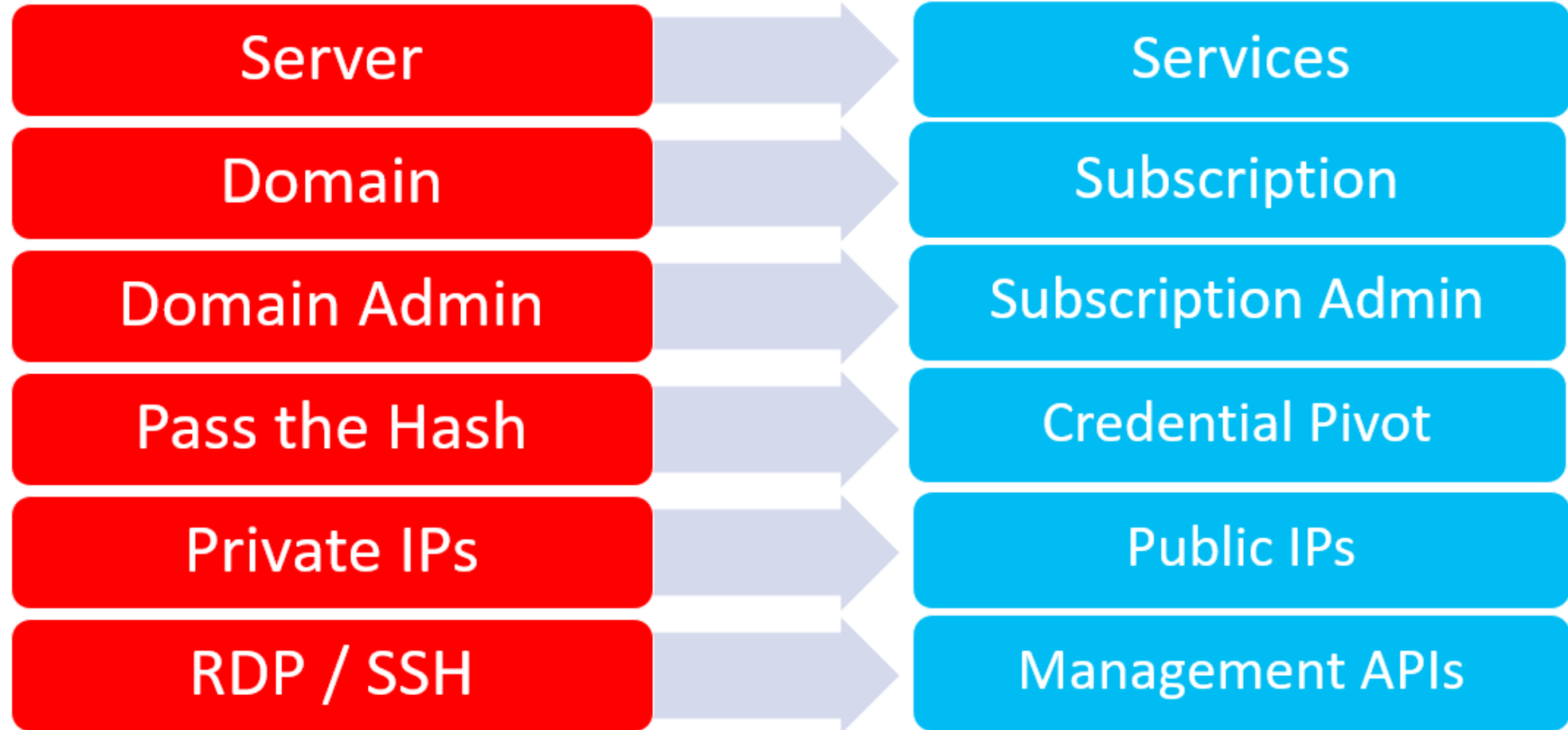
On-Prem

- Purchase, Install, Configure, Deploy:
 - Hardware
 - Software
 - Network
 - Storage
 - Power
 - HVAC
 - Etc...

Cloud

- Pay a metered or monthly fee.
- Responsibility depends on service(s) provided.
- Management & Security capability dependent on provider.

From On-Premises to Cloud



Faust and Johnson – Cloud Post Exploitation Techniques Infiltrate 2017 <https://vimeo.com/214855977>

Cloud Security Challenges



Challenges

- Security controls: On-prem vs cloud
- Cloud environment is constantly changing.
- Rapid changes often mean learning curve is steeper.
- Security capability and best practices depend on Cloud service offering.
- Sharing data appropriately and securely.
- What services and data is private vs what's public isn't always obvious.

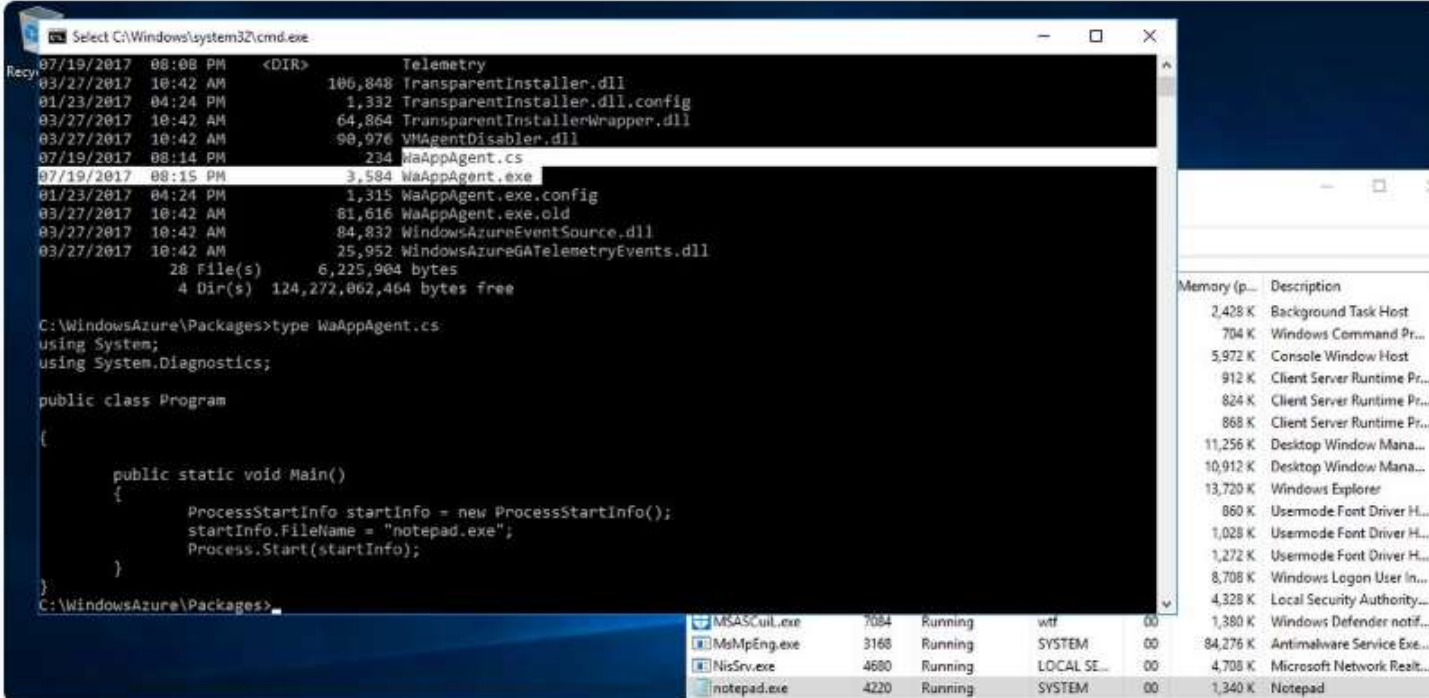
Managing VMs is Still Your Responsibility...

 **Casey Smith** @subTee

If you have #Azure, better check your C:\WindowsAzure folder for RW permissions for NORMAL users. Filed this with MSRC months ago.

#PrivEsc <https://pbs.twimg.com/media/DFH8yMKUIAAOI1h.jpg>

 Twitter | Jul 19th at 1:18 PM (118kB) ▼



```
Select C:\Windows\system32\cmd.exe
07/19/2017 08:08 PM <DIR> Telemetry
03/27/2017 10:42 AM 106,848 TransparentInstaller.dll
01/23/2017 04:24 PM 1,332 TransparentInstaller.dll.config
03/27/2017 10:42 AM 64,864 TransparentInstallerWrapper.dll
03/27/2017 10:42 AM 90,976 VMAGENTDisabler.dll
07/19/2017 08:14 PM 234 WaAppAgent.cs
07/19/2017 08:15 PM 3,584 WaAppAgent.exe
01/23/2017 04:24 PM 1,315 WaAppAgent.exe.config
03/27/2017 10:42 AM 81,616 WaAppAgent.exe.old
03/27/2017 10:42 AM 84,832 WindowsAzureEventSource.dll
03/27/2017 10:42 AM 25,952 WindowsAzureGATelemetryEvents.dll
28 File(s) 6,225,904 bytes
4 Dir(s) 124,272,062,464 bytes free

C:\WindowsAzure\Packages>type WaAppAgent.cs
using System;
using System.Diagnostics;

public class Program
{
    public static void Main()
    {
        ProcessStartInfo startInfo = new ProcessStartInfo();
        startInfo.FileName = "notepad.exe";
        Process.Start(startInfo);
    }
}

C:\WindowsAzure\Packages>
```

Process Name	Private Bytes	Working Set	Session	Architecture	Company Name
MSASvc.exe	7084	Running	wt	00	
MsMpEng.exe	3168	Running	SYSTEM	00	Antimalware Service Executable
NisSrv.exe	4680	Running	LOCAL SE...	00	Microsoft Network Resiliency
notepad.exe	4220	Running	SYSTEM	00	Notepad



Kevin Beaumont @GossiTheDog · Mar 24

Microsoft have a website called docs.com where Office 365 customers can share anything in public. It has a search function.

gslevel	Ticket	Description
0262.02	ST-9124034	Solution: No reoccurrence... Closing
0262.01	ST-9121877	We can not connect to SAP. Solution: ISP fix
0262.02	ST-9122081	check forward configuration for DE Solution: Forward all call wieder ke
0262.06	BPSCS cpanel: le un: pw:	
0262.02	rebecca	
0262.02	C=Qh0-DL	
0262.02	SPARKPOST SMTP PASSWORD:	
0262.02		

<https://>

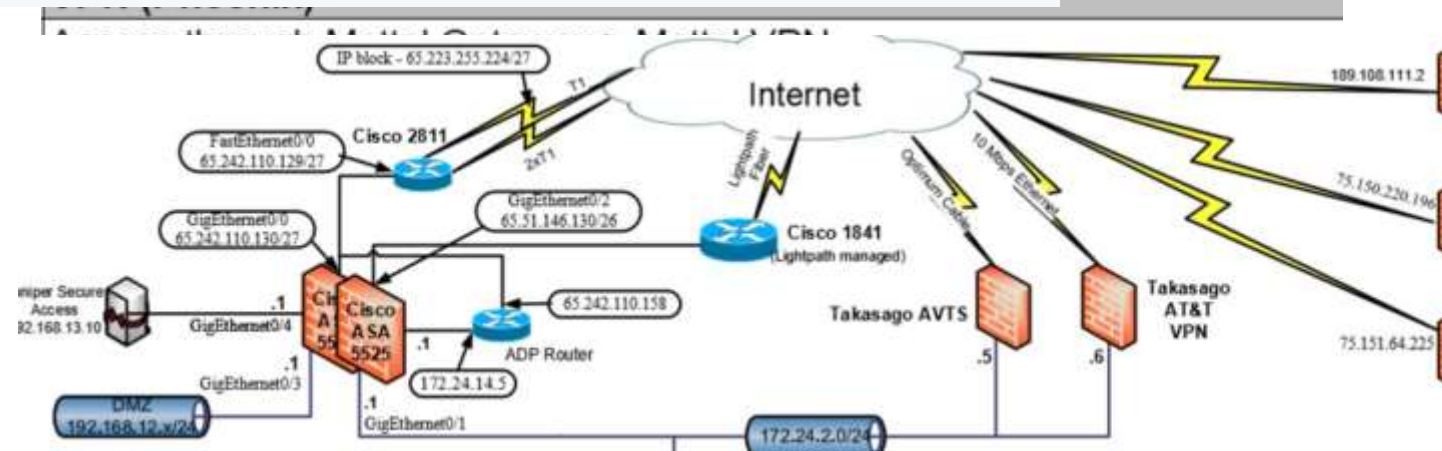
Here you have your account login detail

Hostname:

Username:

Password:

Sean Metcalf (@PyroTek3) TrimarcSecurity.com



Etime - NEW HIRES (INITIAL PASSWORD) LAST 4 DIGITS OF YOUR SS

<https://adpeet2.adp.com/63matp/applications/wtk/html/ess/login.jsp>

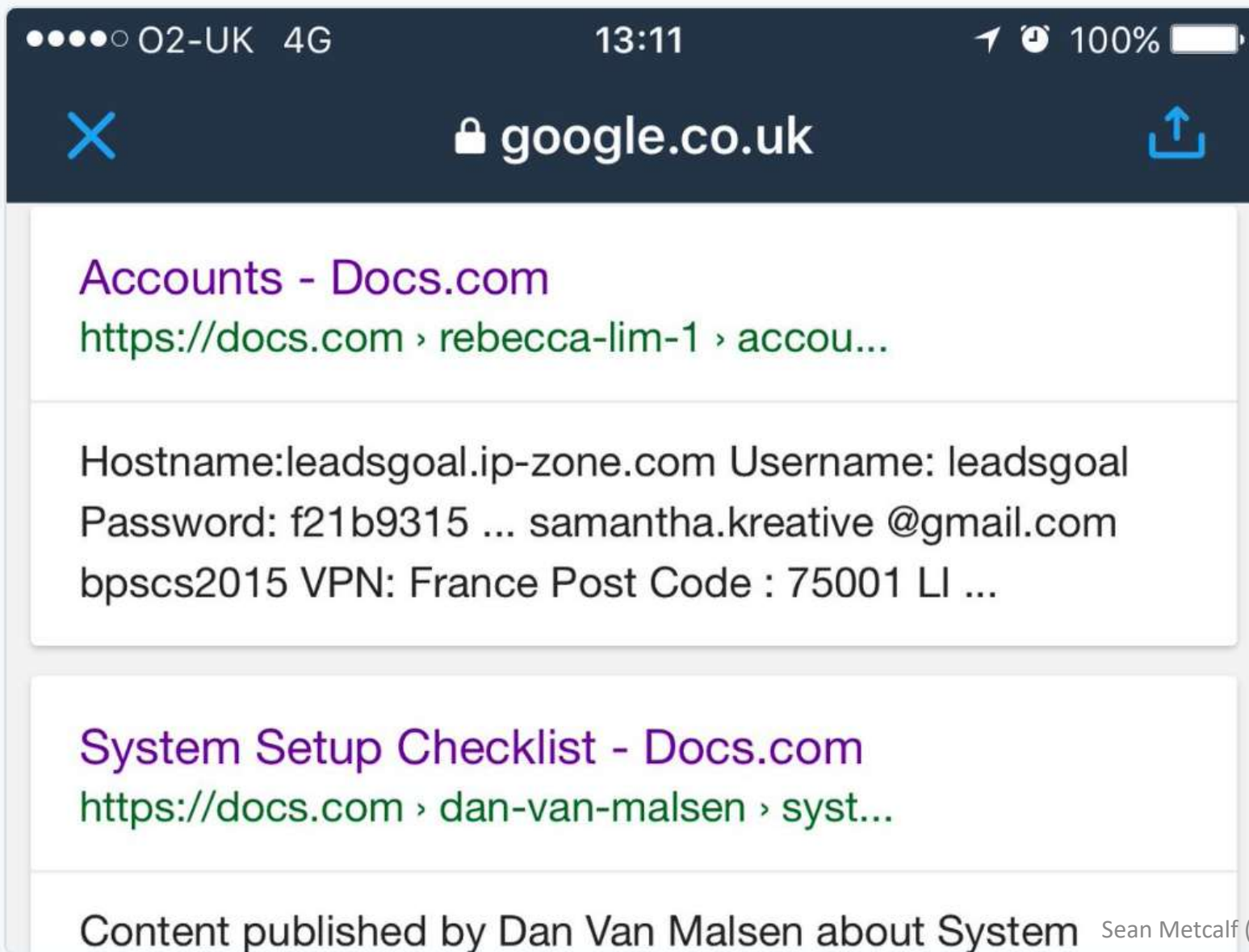
NEW!

Links Disabled Links to external workbooks are not supported and have been disabled.					
	A	B	C	D	E
100	96	19.01.2016		PODM1516-0075	₹ 5,682.00
101	97	12.01.2016		PODM1516-0073	₹ 2,268.00
102	98	05.02.2016		PODM1516-0081	₹ 5,611.00
103	99	05.02.2016		PODM1516-0081	₹ 5,906.00
104	100	08.01.2015		PODM1516-0071	₹ 128,749.00
105	101	25.01.2016/27.01.2016		PODM1516-0078 Rev-1	₹ 47,134.00
106	102	25.01.2016		PODM1516-0078	₹ 49,969.00
107	103	01.02.2016		PODM1516-0080	₹ 7,238.00
108	104	01.02.2016		PODM1516-0079	₹ 1,814.00
109	105	01.02.2016		PODM1516-0079	₹ 1,764.00
110	106	12.01.2016/19.01.2016		PODM1516-0074 Rev-1	₹ 10,223.00



Kevin Beaumont  @GossiTheDog · Mar 26

Google still index docs.com. In fairness to Docs team it clearly says Publicly Viewable when publishing content.



Thank you for using Docs.com. You are receiving this email because you have published content using the service.

Docs.com lets users showcase and share their content with the world. This makes public content easily discoverable via search engines and reusable to others.

We want to make sure that your published content is shared with your intended audience. To review and update the settings, we encourage you to take a few moments to sign in to your account <https://docs.com/me>. For instructions on how to control the privacy

Important information about Docs.com end of service

Applies To: Docs.com

This article was last updated on July 25, 2017

Microsoft's Docs.com service to be discontinued

Microsoft is retiring the [Docs.com](#) service on **Friday, December 15, 2017** and we are hereby advising all users to move their existing Docs.com content to other file storage and sharing platforms as soon as possible, as Docs.com will no longer be available after this date.

There are a number of alternate content sharing options available today. For most Docs.com content, OneDrive represents the ideal platform for sharing your Word, PowerPoint, and PDF content, and offers additional tools, permission settings, and security to help share and protect your data and content. SlideShare from LinkedIn also allows users to share content publicly with its audience of 70 million professionals and vast content library. With the retirement of the Docs.com service, we hope to streamline our offerings in this space and provide you with a more cohesive experience.

We appreciate your patronage of our service and apologize for any inconvenience resulting from this transition. We are happy to provide automatic backup of compatible files to OneDrive and OneDrive for Business.

Please carefully read the information in this article to learn more about your options for transferring or deleting your existing Docs.com content and account.

AUTO LENDER EXPOSES LOAN DATA FOR UP TO 1 MILLION APPLICANTS

Cloud Security Failure: Millions
of Wrestling Fans' Personal
Data Exposed

Amazon S3 Users Exposing
Sensitive Data, Study Finds

**S3 data exposure highlights security
risks in the cloud**

14M Verizon customer records exposed on Amazon
server

**US defense contractor secures Amazon S3 bucket
after leaving sensitive data publicly exposed**

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Whoops! Sensitive intelligence data potentially disclosed...

LILY HAY NEWMAN SECURITY 07.15.17 08:00 AM

BLAME HUMAN ERROR FOR WWE AND VERIZON'S MASSIVE DATA EXPOSURES

Sean Metcalf (@PyroTek3) TrimarcSecurity.com



Jackie Stokes @find_evil

Thanks @awscloud! #infosec <https://pbs>



Twitter | Jul 19th at 7:00 AM (130kB) ▼

to: [Jackie Stokes](#)

[Link](#)

Securing Amazon S3 Buckets [AWS Account:

Today at 04:50

Hello,

We're writing to remind you that one or more of your Amazon S3 bucket access control lists (ACLs) are currently configured to allow access from any user on the Internet. The list of buckets with this configuration is below.

By default, S3 bucket ACLs allow only the account owner to read contents from the bucket; however, these ACLs can be configured to permit world access. While there are reasons to configure buckets with world read access, including public websites or publicly downloadable content

AWS S3 Misconfiguration Explained – And How To Fix It



“If you are vulnerable, attackers could get full access to your S3 bucket, allowing them to download, upload and overwrite files.”

<https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/>

Cloud Discovery: What can we find?



Cloud Recon: DNS MX Records

- Microsoft Office 365:
DOMAIN-COM.mail.protection.outlook.com
- Google Apps (G Suite):
*.google OR *.googlemail.com
- Proofpoint (pphosted)
- Cisco Email Security (iphmx)
- Cyren (ctmail)
- GoDaddy (secureserver)
- CSC (cscdns)

Name	Value
----	-----
outlook.com	116
pphosted.com	110
message1abs.com	46
iphmx.com	34
ctmail.com	29
secureserver.net	25
cscdns.net	18
mimecast.com	18
google.com	15
m1bp.com	6
mb5p.com	6
googlemail.com	6
barracudanetworks.com	6

Cloud Recon: DNS TXT Records

MS = Microsoft Office 365

Google-Site-Verification = G Suite

Amazonses = Amazon Simple Email

OSIAGENTREGURL = Symantec MDM

AzureWebsites = Microsoft Azure

Paychex = Paychex financial services

Docusign = Docusign digital signatures

Atlassian-* = Atlassian services

Name	Value
-----	-----
MS	535
google-site-verification	242
adobe-idp-site-verification	86
docusign	80
v	54
globalsign-domain-verification	47
amazonses	31
atlassian-domain-verification	16
cisco-ci-domain-verification	11
dropbox-domain-verification	9
yandex-verification	6
OSIAGENTREGURL	6
bugcrowd-verification	4
cisco-site-verification	4
ios-enroll	3
have-i-been-pwned-verification	3
azurewebsites	3
android-mdm-enroll	2
status-page-domain-verifica...	2
android-enroll	2
paychex	1
Type	1
OLDMS	1
domain-verification	1
archiva-site-verification	1

Cloud Recon: SPF Records

SalesForce (salesforce.com, pardot.com, & exacttarget.com)

MailChimp (mcsv.net)

Mandrill (MailChimp paid app)

Q4Press (document collaboration)

Zendesk (support ticket)

Oracle Marketing (Eloqua.com)

Constant Contact (email marketing)

Postmark (mtasv.net)

Name	Value
-----	-----
protection.outlook	180
pphosted.com	71
messagelabs.com	41
google.com	30
salesforce.com	30
mandrillapp.com	19
mcsv.net	19
pardot.com	17
q4press.com	16
exacttarget.com	12
mimecast.com	9
zendesk.com	8
oracle.com	8
eloqua.com	7
boardbooks.com	6
spf.messagelabs	6
qualtrics.com	5
clearslide.com	5
clickdimensions.com	5
constantcontact.com	4
satmetrix.com	4
microsoft.com	4
amazon.com	4

Discover Federation Servers

No standard naming for FS.

Some are hosted in the cloud.

DNS query for:

- adfs
- auth
- fs
- okta
- ping
- sso
- sts

```
Name       : adfs.██████████.com
QueryType  : A
TTL        : 299
Section    : Answer
IP4Address : ██████████

Name       : sso.██████████.com
QueryType  : A
TTL        : 899
Section    : Answer
IP4Address : ██████████

Name       : sts.██████████.com
QueryType  : A
TTL        : 86399
Section    : Answer
IP4Address : ██████████

Name       : okta.██████████.com
QueryType  : CNAME
TTL        : 299
Section    : Answer
NameHost   : ██████████.okta.com

Name       : ██████████.okta.com
QueryType  : CNAME
TTL        : 299
Section    : Answer
NameHost   : hammer-crtrs.okta.com

Name       : hammer-crtrs.okta.com
QueryType  : A
TTL        : 299
Section    : Answer
IP4Address : ██████████
```


Federation Web Page Detail

```
{[Accept-Ranges, bytes], [Content-Length, 2631], [Content-Type, t
{[X-FRAME-OPTIONS, DENY], [Content-Language, en-US], [X-Content-T
{[X-Akamai-Transformed, 9 20 0 pmb=mTOE,1], [Connection, keep-ali
{[Vary, X-FORWARDED-FOR], [Strict-Transport-Security, max-age=315
{[content-language, en-us], [transfer-encoding, chunked], [access
{[Vary, user-agent], [Connection, keep-alive], [Content-Length, 4
{[Vary, user-agent], [Connection, keep-alive], [Content-Length, 4
{[Content-Language, en-US], [EC2-instance-id, i-aa8ef952], [Pragm
{[Accept-Ranges, bytes], [Content-Length, 2631], [Content-Type, t
{[Content-Language, en-US], [EC2-instance-id, i-aa8ef952], [Pragm
{[Pragma, no-cache], [AM_CLIENT_TYPE, genericHTML], [Cache-Contro
{[Vary, user-agent], [Connection, keep-alive], [Content-Length, 4
{[Accept-Ranges, bytes], [Content-Length, 215], [Content-Type, te
{[Vary, X-FORWARDED-FOR], [Strict-Transport-Security, max-age=315
{[pragma, no-cache], [Content-Length, 9082], [Cache-Control, no-c
{[Accept-Ranges, bytes], [Content-Length, 689], [Content-Type, te
{[X-FRAME-OPTIONS, DENY], [Content-Language, en-US], [X-Content-T
{[Accept-Ranges, bytes], [Content-Length, 689], [Content-Type, te
{[pragma, no-cache], [Content-Length, 9082], [Cache-Control, no-c
{[Connection, close], [X-Frame-Options, DENY], [Pragma, no-cache]
{[Pragma, no-cache], [AM_CLIENT_TYPE, genericHTML], [Cache-Contro
{[Pragma, no-cache], [x-frame-options, DENY], [Content-Length, 12
{[Accept-Ranges, bytes], [Content-Length, 689], [Content-Type, te
```

Apache
Apache-Coyote/1.1
BigIP
JPMM
Kestrel
Microsoft-HTTPAPI/2.0 Microsoft-HTTPAPI/2.0
Microsoft-IIS/7.5
Microsoft-IIS/7.5,Microsoft-IIS/6.0
Microsoft-IIS/7.5,Microsoft-IIS/7.5
Microsoft-IIS/8.0
Microsoft-IIS/8.5
Microsoft-IIS/8.5 Microsoft-HTTPAPI/2.0
nginx
Oracle-iPlanet-web-Server/7.0
webSEAL/7.0.0.8 (Build 160317)

TiPMix=0.505320029568542; path=/; Domain=okta. [REDACTED], ARR

En1L; expires=Wed, 11-Oct-2017 17:06:46 GMT; Max-Age=7776000; path=/; domain=

Federation Server Certificate Info



Server Key and Certificate #1

Subject	Fingerprint SHA256: 152151b387412a95ab9f Pin SHA256: hUIG87ch71EZQYhZBEkg2VKE
Common names	
Alternative names	
Serial Number	0c0099b7d789c9f6f
Valid from	Fri, 09 Dec 2016 00:00:00 UTC
Valid until	Thu, 25 Jan 2018 12:00:00 UTC (expires in 11 months)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	DigiCert SHA2 High Assurance Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.cer
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL: OCSP CRL: http://crl3.digicert.com/sha2-ha-server-g5.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes

Configuration



Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.



Cipher Suites

# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 ^P
OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 ^P

Federation Server Compromise

How to steal identities – federated style

Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

Token & Signing certificates \sim KRBTGT (think Golden Tickets)

DEF CON 25 (July 2017)



Similar to a [golden ticket attack](#), if we have the key that signs the object which holds the user's identity and permissions (*KRBtgt* for golden ticket and token-signing private key for golden SAML), we can then forge such an "authentication object" (TGT or SAMLResponse) and impersonate any user to gain unauthorized access to the SP. Roger Grimes [defined](#) a golden ticket attack back in 2014 not as a Kerberos tickets forging attack, but as a Kerberos Key Distribution Center (KDC) forging attack. Likewise, a golden SAML attack can also be defined as an IdP forging attack.

In this attack, an attacker can control every aspect of the SAMLResponse object (e.g. username, permission set, validity period and more). In addition, golden SAMLs have the following advantages:

- They can be **generated** from practically **anywhere**. You don't need to be a part of a domain, federation of any other environment you're dealing with
- They are effective even when **2FA** is enabled
- The token-signing **private key** is **not renewed** automatically
- Changing a user's password won't affect the generated SAML

<https://www.cyberark.com/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-cloud-apps/>

PowerShell Management of Cloud Stuff

- Amazon AWS
<https://aws.amazon.com/powershell/>
- Google Cloud
<https://cloud.google.com/powershell/>
- Microsoft Azure
<https://docs.microsoft.com/en-us/powershell/azure/install-azurermps?view=azurermps-4.1.0>
- Microsoft Office 365
<https://technet.microsoft.com/en-us/library/dn975125.aspx>
- Azure Cloud Shell (in browser BASH or PowerShell shell)


```
PS C:\windows\system32> Get-MSolCompanyInformation

DisplayName      : International Genetic Technologies
PreferredLanguage : en
Street           : 100 Farallon Road
City             : Palo Alto
State            : CA
Postalcode       : 94301
Country          : 
CountryLetterCode : US
TelephoneNumber  : (415) 209-5451
MarketingNotificationEmails : {}
TechnicalNotificationEmails : {johnarnold@ingentch.co}
SelfServePasswordResetEnabled : True
UsersPermissionToCreateGroupsEnabled : True
UsersPermissionToCreateLOBAppsEnabled : True
UsersPermissionToReadOtherUsersEnabled : True
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled : True
DirSyncServiceAccount : 
LastDirSyncTime  : 
LastPasswordSyncTime : 
PasswordSynchronizationEnabled : False
```

Get-MSolGroup			
objectId	DisplayName	GroupType	Description
-----	-----	-----	-----
912f339b-a375-4747-8fe6-c5957e9e93a3	InGen Systems Admins	Security	Unix System Admins
12579f60-0287-4ac6-a0d5-89ce5312a8f4	InGen Security	Security	Security Team
6a4e110c-5434-4586-876b-34b529432ace	InGen R&D	Security	R&D
26248498-4769-4e3f-b164-94255de18e4c	InGen Dino Team	Security	Dino Team
a3de767a-f0f4-4b2a-ac1d-0d0160358dec	AAD DC Administrators	Security	
868545b6-1579-45e2-8839-ab68e0ab6017	Password Reset Group	Security	
af72c0d8-f19f-48ba-a6c6-0cbda7d0846f	InGenPasswordResetGroup	Security	

Name	AvailabilityStatus	AuthenticationType
----	-----	-----
starkindustriestech.net		Managed
cyberdynesys.net		Managed
ingentech.co		Managed


AAD – Microsoft Graph Explorer

The screenshot displays the Microsoft Graph Explorer interface. On the left sidebar, the 'Authentication' section indicates a sample account is used, with a 'Sign in with Microsoft' button. Below it, the 'Sample Queries' section lists various queries under 'Users' and 'Groups' categories, each with a method (GET or POST) and a brief description. The main area shows a GET request to the URL `https://graph.microsoft.com/v1.0/groups` with a status of 'Success - Status Code 200' and a response time of '603ms'. The 'Response Preview' tab is active, displaying a JSON response for a group. The JSON includes details such as group types, email address, mail enabled status, and group description.

Graph Explorer

Authentication

You are currently using a sample account. To access your own data:

 Sign in with Microsoft

Sample Queries

Users

- GET my direct reports
- GET all users in the organization
- GET all users in the Finance depart...
- GET my skills
- GET user by email
- GET all my Planner tasks
- POST create user
- GET track user changes

Groups

- GET all groups in my organization
- GET all groups I belong to
- GET group members

GET v1.0 `https://graph.microsoft.com/v1.0/groups` Run Query

Request Body Request Headers

Key Value

Enter new header

Success - Status Code 200 603ms

Response Preview Response Headers

```
{
  "groupTypes": [
    "Unified"
  ],
  "mail": "BusinessDevelopment@M365x214355.onmicrosoft.com",
  "mailEnabled": true,
  "mailNickname": "BusinessDevelopment",
  "onPremisesLastSyncDateTime": null,
  "onPremisesProvisioningErrors": [],
  "onPremisesSecurityIdentifier": null,
  "onPremisesSyncEnabled": null,
  "preferredDataLocation": null,
  "proxyAddresses": [
    "SMTP:BusinessDevelopment@M365x214355.onmicrosoft.com"
  ],
  "renewedDateTime": "2017-07-31T18:56:22Z",
  "securityEnabled": false,
  "visibility": "Private"
},
{
  "id": "14d0da09-90ed-4ec6-a7b1-8e234e542fff",
  "deletedDateTime": null,
  "classification": null,
  "createdDateTime": "2017-07-31T17:36:54Z",
  "description": "Quality Assurance group forum to discuss bugs, fixes, and obstacles to releasing the best products in the marketplace",
  "displayName": "Quality Assurance",
```

<https://developer.microsoft.com/en-us/graph/graph-explorer#>

PSMSGraph <https://github.com/markekraus/PSMSGraph>

This is a PowerShell module API wrapper for the Microsoft Graph API.

What is Microsoft Graph?

The [Microsoft Graph API](#) is a REST API provided by Microsoft for integrating and managing Office 365 Exchange Online, OneDrive for Business, and Azure AD. It allows for application developers to integrate their apps with those Microsoft Services. Management of the environment is also possible but requires understanding of OAuth and REST.

Why use the PSMSGraph module?

This module is an API wrapper. It seeks to take the "foreign" concepts of REST and OAuth and make them accessible and usable in PowerShell. This module strives to make PowerShell administration and automation tasks via the Microsoft Graph API more like other PowerShell commands.

Features

- In-memory and at-rest security of the Access Token, Refresh Token, and Client Secret. These are all stored in memory as secure strings and are only made plain-text on demand when needed. When exported to disk, they are done so with CLI XML which maintains the secure string.
- Extensible type (Mark's "Poor Man's Classes") system allow for piping between functions similar to Active Directory or Exchange cmdlets
- Easy OAuth authorization process with a WinForms authentication popup
- No "mystery DLL's" required. The entire OAuth authorization, token request, and token refresh process is written in pure PowerShell
- Export and Import access tokens between sessions allowing you to authorize an application once and reuse the token until the refresh expires from lack of use or is revoked. Great for automation!
- No hassle Token Refreshing!! Calls to `Invoke-GraphRequest` (and all the functions that utilize it) automatically track the

Identity Management in the Cloud (Active Directory)



Azure “Active Directory”

On-premises Active Directory

- Authentication, Directory, & Management
- AD Forest for single entity
- Internal corporate network
- Authentication
 - Kerberos
 - NTLM
- LDAP
- Group Policy

Azure AD (Office 365)

- Identity
- Designed for multi-tenant
- Cloud/web-focused
- Authentication
 - SAML 2.0
 - OpenID Connect
 - OAuth 2.0
 - WS-Federation
- REST API: AD Graph API

Active Directory & the Cloud

- AD provides Single Sign On (SSO) to cloud services.
- Some directory sync tools synchronizes all users & attributes to cloud service(s).
- Most sync engines only require AD user rights to send user and group information to cloud service.
- Most organizations aren't aware of all cloud services active in their environment.
- **Do you know what cloud services sync information from your Active Directory?**

Azure AD Connect

- **Filtering** – select specific objects to sync (default: all users, contacts, groups, & Win10). Adjust filtering based on domains, OUs, or attributes.
- **Password synchronization** – AD pw hash hash ---> Azure AD.
PW management only in AD (use AD pw policy)
- **Password writeback** - enables users to update password while connected to cloud resources.
- **Device writeback** – writes Azure AD registered device info to AD for conditional access.
- **Prevent accidental deletes** – protects against large number of deletes (enabled by default).
feature is turned on by default and protects your cloud directory from numerous deletes at the same time. By default it allows 500 deletes per run. You can change this setting depending on your organization size.
- **Automatic upgrade** – Keeps Azure AD Connect version current (express settings enabled by default).

Express Permissions for Azure AD Connect

Permissions for the created AD DS account for express settings

The [account](#) created for reading and writing to AD DS have the following permissions when created by express settings:

Permission	Used for
<ul style="list-style-type: none">• Replicate Directory Changes• Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

Express Permissions for Azure AD Connect

Permissions for the created AD DS account for express settings

The [account](#) created for reading and writing to AD DS have the following permissions when created by express settings:

DEF CON 25 (July 2017)



Permission	Used for
<ul style="list-style-type: none">• Replicate Directory Changes• Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

DCSync

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN          : Administrator

** SAM ACCOUNT **

SAM Username       : Administrator
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration  :
Password last change : 9/7/2015 9:54:33 PM
Object Security ID  : S-1-5-21-2578996962-4185879466-3696909401-500
Object Relative ID  : 500

Credentials:
  Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fda365d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236ed3f3ac
    lm - 0: 6cfd3c1bcc30b3fe5d716fef10f46e49
    lm - 1: d1726cc03fb143869304c6d3f30fdb8d

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
  Default Salt : RD.ADSECURITY.ORGAdministrator
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638deac142e3674af58a674b67e102b
    aes128_hmac      (4096) : f4d4892350fbc545f176d418afabf2b2
    des_cbc_md5      (4096) : 5d8c9e46a4ad4acd
    rc4_plain        (4096) : 96ae239ae1f8f186a205b6863a3c955f
  OldCredentials
    aes256_hmac      (4096) : 0526e75306d2090d03f0ea0e0f681aae5ae591e2d9c27ea49c3322525382dd3f
    aes128_hmac      (4096) : 4c41e4d7a3e932d64feeed264d48a19e
    des_cbc_md5      (4096) : 5bfd0d0efe3e2334
    rc4_plain        (4096) : 5164b7a0fda365d56739954bbbc23835
```

Custom Permissions for Azure AD Connect

Feature	Permissions
msDS-ConsistencyGuid feature	Write permissions to the msDS-ConsistencyGuid attribute documented in Design Concepts - Using msDS-ConsistencyGuid as sourceAnchor .
Password sync	<ul style="list-style-type: none">• Replicate Directory Changes• Replicate Directory Changes All
Exchange hybrid deployment	Write permissions to the attributes documented in Exchange hybrid writeback for users, groups, and contacts.
Exchange Mail Public Folder	Read permissions to the attributes documented in Exchange Mail Public Folder for public folders.
Password writeback	Write permissions to the attributes documented in Getting started with password management for users.
Device writeback	Permissions granted with a PowerShell script as described in device writeback .
Group writeback	Read, Create, Update, and Delete group objects in the OU where the distributions groups should be located.

Microsoft Security Advisory 4056318

Guidance for securing AD DS account used by Azure AD Connect for directory synchronization

Published: December 12, 2017

Version: 1.0

Executive Summary



Microsoft is releasing this security advisory to provide information regarding security settings for the AD DS (Active Directory Domain Services) account used by Azure AD Connect for directory synchronization. This advisory also provides guidance on what on-premises AD administrators can do to ensure that the account is properly secured.

Advisory Details

[Azure AD Connect](#) lets customers synchronize directory data between their on-premises AD and Azure AD. Azure AD Connect requires the use of an AD DS user account to access the on-premises AD. This account is sometimes referred to as the AD DS connector account. When setting up Azure AD Connect, the installing administrator can either:

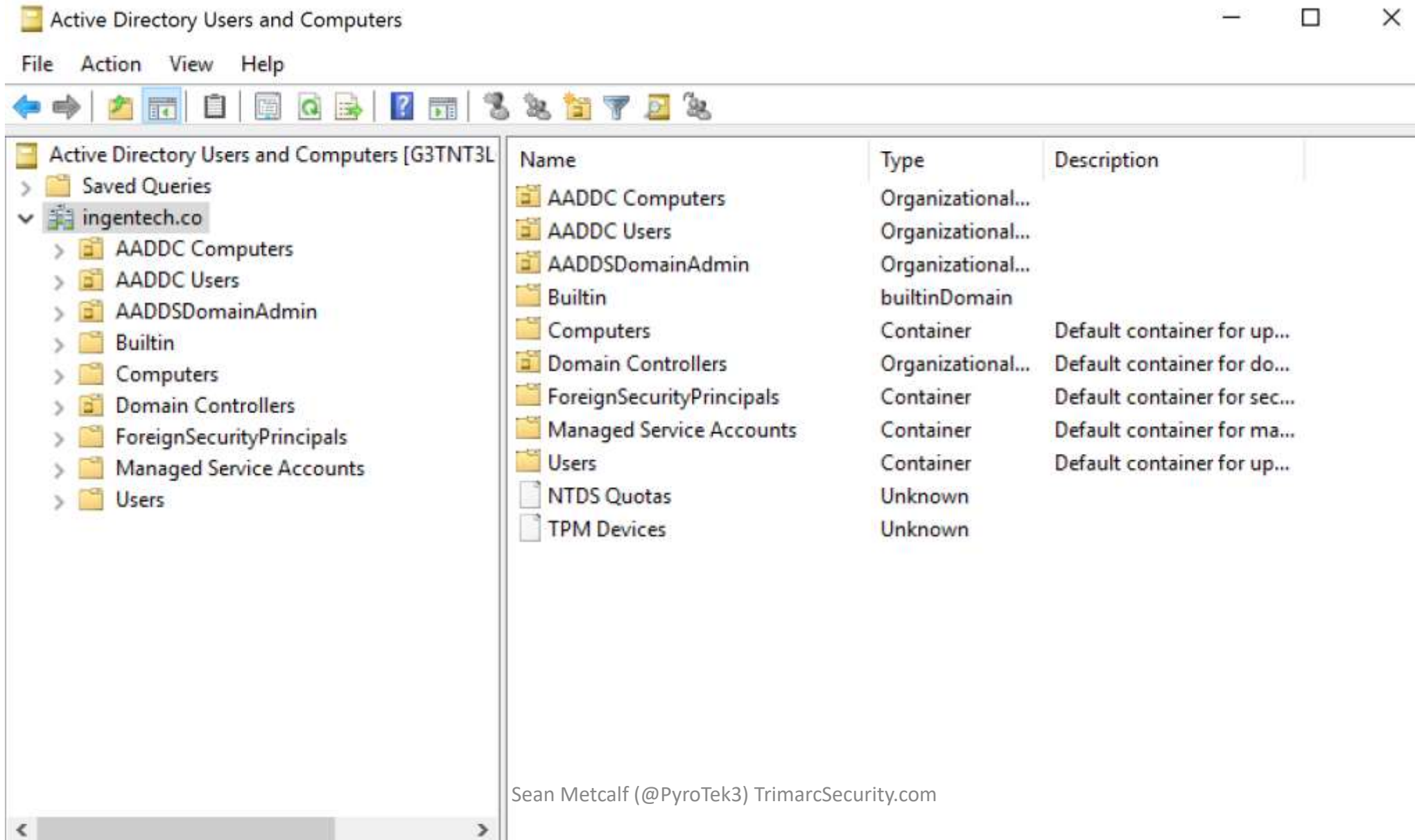
- Provide an existing AD DS account, or
- Let Azure AD Connect automatically create the account. The account will be created directly under the on-premises AD User container. For Azure AD Connect to fulfill its function, the account must be granted specific privileged directory permissions (such as Write permissions to directory objects for Hybrid Exchange writeback, or DS-Replication-Get-Changes and DS-Replication-Get-Changes-All for Password Hash Synchronization). To learn more about the account, refer to article [Azure AD Connect: Accounts and Permissions](#).

<https://technet.microsoft.com/en-us/library/security/4056318.aspx>

Microsoft: Azure AD Domain Services

- Active Directory managed by Microsoft in the cloud.
- “AD as a Service”
- Custom names
- Domain-join support
- Integrated with Azure AD
- NTLM & Kerberos auth support
- Group Policy
- AD management tools supported
- AAD DC Administrators, not Domain/Enterprise Admins

Microsoft: Azure AD Domain Services



Microsoft: Azure AD Domain Services

- No Capability:
 - Schema updates (no LAPS)
 - LDAP writes
 - Trusts
 - Domain Controller direct access
 - Modification of domain & DC policies
- Federation capability through Azure AD
- Connectivity with on-prem AD is limited
- Object & pw sync through Azure AD Connect
 - Sync from on-prem to Azure AD
 - Sync from Azure AD to Azure AD DS

Amazon AWS Active Directory

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [WIN-C]

- > Saved Queries
- ▼ ad.cyberdynesys.net
 - AWS Delegated Groups
 - AWS Reserved
 - Builtin
 - Computers
 - ▼ CYBERDYNE
 - Computers
 - Users
 - Domain Controllers
 - > ForeignSecurityPrincipals
 - > Managed Service Accounts
 - Users

Name	Type	Description
Admins	Security Group...	Legacy Administrators G...
AWS Delegated Account Operators	Security Group...	AWS Provided Group: M...
AWS Delegated Add Workstations To Domain Users	Security Group...	AWS Provided Group: M...
AWS Delegated Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Domain Name System Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Dynamic Host Configuration Protocol Admin...	Security Group...	AWS Provided Group: M...
AWS Delegated Enterprise Certificate Authority Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Fine Grained Password Policy Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Group Policy Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Kerberos Delegation Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Managed Service Account Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Remote Access Service Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Replicate Directory Changes Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Server Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Sites and Services Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated Terminal Server Licensing Administrators	Security Group...	AWS Provided Group: M...
AWS Delegated User Principal Name Suffix Administrators	Security Group...	AWS Provided Group: M...

Hybrid Identity Protection Conference 2017

Amazon AWS Directory (Active Directory)	Microsoft Azure AD Domain Services
Windows Server 2012 R2 DFL/FFL	Windows Server 2012 R2 DFL/FFL
Designed for Cloud and Corporate workloads.	Designed for Azure VM joins (primarily).
Support for trusts including resource forest. Schema updates supported (LDIF import).	Trusts are not supported. No schema updates.
Ability to spin up additional DCs in different geographic locations.	Standard 2 DCs in a single virtual network in Azure
Password sync not supported.	Supports password sync from production AD.
5 Fine-grained Password Policies available for modification to manage password policies.	Not supported.
O365 integration support: install Azure AD Connect, ADFS, etc.	Integration with Azure AD.
Domain join at VM instance creation.*	
Pricing: ~\$80 - \$280/month	Pricing: ~\$80 - \$100/month

Exploit Scenarios

Attacking Office 365




Gathering Email Content from O365

- MailSniper can connect to on-prem Exchange and O365 to pull data from mailboxes.

```
PS C:\> Invoke-SelfSearch -Remote -ExchHostname outlook.office365.com
cmdlet Invoke-SelfSearch at command pipeline position 1
Supply values for the following parameters:
Mailbox: jhammond@ingentech.co
[*] Trying Exchange version Exchange2010
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
[*] Using EWS URL https://outlook.office365.com/EWS/Exchange.asmx
[***] Found folder: Inbox
[*] Now searching mailbox: jhammond@ingentech.co for the terms *password* *creds* *credentials*.
```

Account 'Backdoor' Access: EWS Crack

EWS Cracker



What's EWS?

EWS stands for Exchange Web Services. This is a SOAP based protocol used for free/busy scheduling, and leveraged by third party clients. It allows a user to read email, send email, test credentials.

Unfortunately, EWS only supports Basic Authentication. If you have multi-factor authentication through a third party provider, such as Ping, Duo or Okta, EWS can be used to bypass MFA. It can also be used to bypass MDM solutions.

This was documented by the fine folks at Black Hills InfoSec as well as by Duo c

Microsoft's official response is to use Microsoft provided MFA, which produce a enourmous amount of O365 customers in a difficult state. Most customers seer

Other fun facts about EWS:

- Logging is not 100%. It may log failed attempts in your audit logs, it may n
- It helpfully provides user enumeration. If a user doesn't exist, a different en

UPDATE as of 11:15am EST on 11/4/16 BHIS has retested the portion of this article detailing a bypass against Office365 Multi-Factor Authentication and it does indeed appear to not work.

Some individuals have pointed out that they were getting 401 Unauthorized error messages when connecting in via EWS with MFA fully enabled on a user. When testing against the initial test user BHIS tested against EWS on O365 it now produces the same 401 error results when using a password to authenticate. BHIS believes that the results obtained previously were due to a delay in which Office365 MFA was denying access to Exchange Web Services after recently enabling it for a user. A video demonstrating this has been put together here: https://youtu.be/Bb_T3ILfIU

Access Defaults



Sean (Trimarc Research)

sean@trimarcresearch.com

Email apps

Choose the apps the user can use to access their Office 365 email.

Outlook on the web



On

Outlook desktop (MAPI)



On

Exchange web services



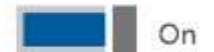
On

Mobile (Exchange ActiveSync)



On

IMAP



On

POP



On

Limiting Access



Sean (Trimarc Research)
sean@trimarcresearch.com

Email apps

Choose the apps the user can use to access their Office 365 email.

Outlook on the web  On

Outlook desktop (MAPI)  On

Exchange web services  Off

Mobile (Exchange ActiveSync)  Off

IMAP  Off

POP  Off

Compromise Single Account to Own the Cloud

- Global Admin is typically the user's email address who signs up for the service.
- This is typically a user account.
- Tends to retain this access.
- Everyone wants Global Admin (it's just the cloud, right?)
- Own this account to own cloud services.

Mitigation:

Protect cloud admins like AD admins.

Cloud Password Reset Ability with Write-back

1. Cloud PW Reset Admin account used to reset cloud account passwords.
2. Cloud PW Reset Admin account is compromised.
3. Azure AD Connect write-back is enabled, so these passwords get updated on the corporate network.
4. Attacker now owns accounts on-premises.

Mitigation:

Ensure on-prem admin accounts are not cloud enabled.

Compromise Azure AD Connect Service Account

1. Gain access to Azure AD Connect account/server
2. Express Permissions/ PW sync enabled provides DCSync capability
3. If PW Sync is enabled, all synced user passwords pass through Azure AD Connect server.

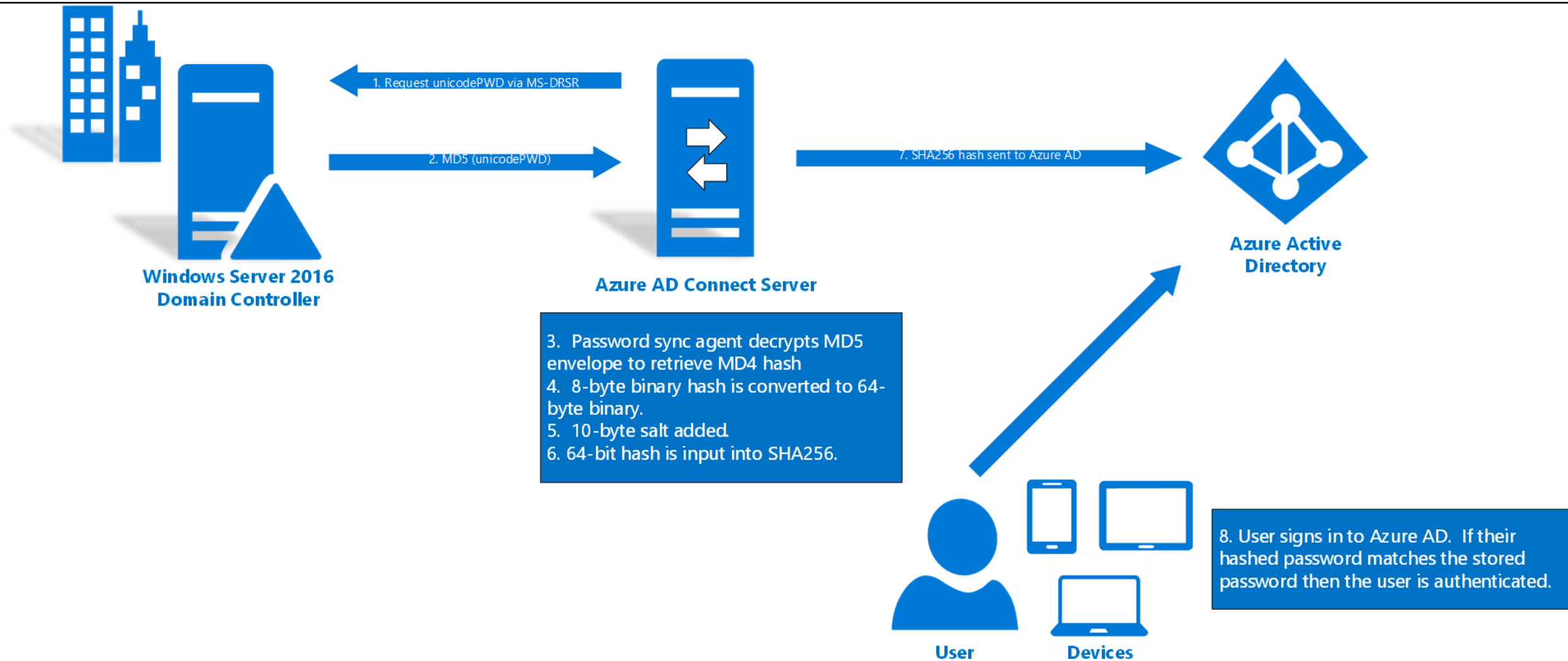
Mitigation:

Ensure only Domain Admins has permissions on this service account.

Compromise Azure AD Connect Server

- If PW Sync is enabled, all synced user passwords pass through Azure AD Connect server.
- *Mitigation:*
Protect this server like a Domain Controller

PW Sync (MD4+salt+PBKDF2+HMAC-SHA256)



Others?

Still researching...

Office 365 Auditing & Logging



Search the audit log in the Office 365 Security & Compliance Center

[Search the audit log](#)

[Before you begin](#)

[Audited activities](#)

[More info](#)

The tables in this section describe the activities that are audited in Office 365. You can search for these events by searching the audit log in the Security & Compliance Center. Click the **Search the audit log** tab for step-by-step instructions.

These tables group related activities or the activities from a specific Office 365 service. The tables include the friendly name that's displayed in the **Activities** drop-down list and the name of the corresponding operation that appears in the detailed information of an audit record and in the CSV file when you export the search results. Click one of the following links to go to a specific table

File and page activities	Folder activities	Sharing and access request activities
Synchronization activities	Site administration activities	Exchange mailbox activities
Sway activities	User administration activities	Azure AD group administration activities
Application administration activities	Role administration activities	Directory administration activities
eDiscovery activities	Power BI activities	Microsoft Teams activities
Yammer activities	Exchange admin activities	

Search the audit log in the Office 365 Security & Compliance Center

[Search the audit log](#)

[Before you begin](#)

[Audited activities](#)

[More info](#)

Be sure to read the following items before you start searching the Office 365 audit log.

- You (or another admin) must first turn on audit logging before you can start searching the Office 365 audit log. To turn it on, just click **Start recording user and admin activity** on the **Audit log search** page in the Security & Compliance Center. (If you don't see this link, auditing has already been turned on for your organization.) After you turn it on, a message is displayed that says the audit log is being prepared and that you can run a search in a couple of hours after the preparation is complete. You only have to do this once.

NOTE: We're in the process of turning on auditing by default. Until then, you can turn it on as previously described.

- You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the Office 365 audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the **Permissions** page in the Exchange admin center. To give a user the ability to search the Office 365 audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only Audit Logs or Audit Logs role, and then add the user as a member of the new role group. For more information, see [Manage role groups in Exchange Online](#).

IMPORTANT: If you assign a user the View-Only Audit Logs or Audit Logs role on the **Permissions** page in the Security & Compliance Center, they won't be able to search the Office 365 audit log. You have to assign the permissions in Exchange Online. This is because the underlying cmdlet used to search the audit log is an Exchange Online cmdlet.

Office 365 Audit Log Data API

- If you want to programmatically download data from the Office 365 audit log, we recommend that you use the Office 365 Management Activity API instead of using a PowerShell script. The Office 365 Management Activity API is a REST web service that you can use to develop operations, security, and compliance monitoring solutions for your organization. For more information, see [Office 365 Management Activity API reference](#).

Enable Office 365 Auditing

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange  
-ConnectionUri https://outlook.office365.com/powershell-liveid/  
-Credential $UserCredential -Authentication Basic -AllowRedirection  
Import-PSSession $Session  
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $True
```

```
PS C:\> Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $True  
  
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled  
WARNING: The admin audit log configuration change you specified could take up to 60 minutes to take effect.  
  
UnifiedAuditLogIngestionEnabled : True
```

Search the audit log in the Office 365 Security & Compliance Center

Search the audit log

Before you begin

Audited activities

More info

Need to find if a user viewed a specific document or purged an item from their mailbox? If so, you can use the Office 365 Security & Compliance Center to search the unified audit log to view user and administrator activity in your Office 365 organization. Why a unified audit log? Because you can search for the following types of user and admin activity in Office 365:

- User activity in SharePoint Online and OneDrive for Business
- User activity in Exchange Online (Exchange mailbox audit logging)

IMPORTANT: Mailbox audit logging must be turned on for each user mailbox before user activity in Exchange Online will be logged. For more information, see [Enable mailbox auditing in Office 365](#).

- Admin activity in SharePoint Online
- Admin activity in Azure Active Directory (the directory service for Office 365)
- Admin activity in Exchange Online (Exchange admin audit logging)
- User and admin activity in Sway
- User and admin activity in Power BI for Office 365
- User and admin activity in Microsoft Teams
- User and admin activity in Yammer

Exchange mailbox activities

The following table lists the activities that can be logged by mailbox audit logging. Mailbox activities performed by the mailbox owner, a delegated user, or an administrator are logged. **By default, mailbox auditing in Office 365 isn't turned on. Mailbox audit logging must be turned on for each mailbox before mailbox activity will be logged.** For more information, see [Enable mailbox auditing in Office 365](#).

Friendly name	Operation	Description
Added delegate mailbox permissions	Add-MailboxPermission	An administrator assigned the FullAccess mailbox permission to a user (known as a <i>delegate</i>) to another person's mailbox. The FullAccess permission allows the delegate to open the other person's mailbox, and read and manage the contents of the mailbox.
Copied messages to another folder	Copy	A message was copied to another folder.
Created or received messages	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 message or folder creation isn't audited.
Deleted messages from Deleted Items folder	SoftDelete	A message was permanently deleted or deleted from the Deleted Items folder. These items are moved to the Recoverable Items folder. Messages are also moved to the Recoverable Items folder when a user selects it and presses Shift+Delete .
Moved messages to another folder	Move	A message was moved to another folder.
Moved messages to Deleted Items folder	MoveToDeletedItems	A message was deleted and moved to the Deleted Items folder.
Purged messages from the mailbox	HardDelete	A message was purged from the Recoverable Items folder (permanently deleted from the mailbox).
Removed delegate mailbox	Remove-MailboxPermission	An administrator removed the FullAccess permission (that was assigned to a delegate) from a person's mailbox. After

O365 Exchange Audit Options

- Auditing Types: Admin, Delegate, & Owner
 - Enable Auditing (standard)
 - Mailbox access, certain admin & delegate actions
 - Administrator with Full Access permission to a user's mailbox is considered a delegate user.
 - Enable mailbox Owner auditing
- Auditing logs are kept for 90 days.
- Admin mailbox access scenarios:
 - Mailbox search using In-Place eDiscovery (Exchange Online) or Content Search (Office 365).
 - Microsoft Exchange Server MAPI Editor.

Admin	Delegate	Owner
Copy		
Create (Calendar, Contacts, Notes, or Tasks)	Create (Calendar, Contacts, Notes, or Tasks)	Create (Calendar, Contacts, Notes, or Tasks)
FolderBind (mailbox open)	FolderBind (mailbox open)	
HardDelete (purged from the Recoverable Items)	HardDelete (purged from the Recoverable Items)	HardDelete (purged from the Recoverable Items)
MessageBind (message viewed in preview pane or opened)		MailboxLogin
Move	Move	Move
MoveToDeletedItems	MoveToDeletedItems	MoveToDeletedItems
SendAs	SendAs	
SendOnBehalf	SendOnBehalf	
SoftDelete	SoftDelete	SoftDelete
Update	Update	Update

Enable Office 365 Mailbox Auditing

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange  
-ConnectionUri https://outlook.office365.com/powershell-liveid/  
-Credential $UserCredential -Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session
```

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq  
"UserMailbox"} | `
```

```
Set-Mailbox -AuditEnabled $true -AuditOwner  
MailboxLogin,HardDelete,SoftDelete
```

```
PS C:\> Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | `
Set-Mailbox -AuditEnabled $true -AuditOwner MailboxLogin,HardDelete,SoftDelete
```

Check Office 365 Mailbox Auditing

- `Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | FL Name,Audit*`

```
Name           : JArnold
AuditEnabled    : True
AuditLogAgeLimit : 90.00:00:00
AuditAdmin      : {Update, Move, MoveToDeletedItems, SoftDelete...}
AuditDelegate   : {Update, SoftDelete, HardDelete, SendAs...}
AuditOwner      : {SoftDelete, HardDelete, MailboxLogin}
```

```
Name           : jhammond
AuditEnabled    : True
AuditLogAgeLimit : 90.00:00:00
AuditAdmin      : {Update, Move, MoveToDeletedItems, SoftDelete...}
AuditDelegate   : {Update, SoftDelete, HardDelete, SendAs...}
AuditOwner      : {SoftDelete, HardDelete, MailboxLogin}
```

Azure AD Logging

Azure Active Directory admin center international genetic technologies > Users and groups - Audit logs

Users and groups - Audit logs
international genetic technologies - Azure Active Directory

Columns Refresh Download Troubleshoot

Category: All Activity Resource Type: All Activity: All
Date Range: 1 Month Target: Enter target name or upn Initiated By (Actor): Enter actor name or upn

Apply

Search to filter items...

DATE	TARGET(S)	INITIATED BY (ACTOR)	ACTIVITY
11/3/2017 10:14:46 AM	User : JArnold@ingentech.co	Microsoft App Access Panel	Update user
11/3/2017 10:14:44 AM	User : JArnold@ingentech.co	Microsoft App Access Panel	Update user
11/3/2017 10:14:42 AM	User : JArnold@ingentech.co	JArnold@ingentech.co	Update user
11/3/2017 10:14:42 AM	User : JArnold@ingentech.co	2ded6005-5629-4595-9f78-2bdb7a1d0d3e	User registered for self-service password reset
11/3/2017 10:13:47 AM	User : JArnold@ingentech.co	Microsoft App Access Panel	Update user

international genetic technologies - Risky sign-ins
Azure Active Directory

Overview Quick start

MANAGE

Last 90 days Download Refresh Add known IP address ranges


RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
Medium	Real-time	Sign-in from unfamiliar location ⓘ	0 of 1	10/24/2017 5:53 PM

Monitor App Registrations


international genetic technologies - App registrations

Azure Active Directory


 Overview


 Quick start

MANAGE

 Users and groups

 Enterprise applications

 Devices (Preview)

 App registrations

 New application registration  Endpoints  Troubleshoot

To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).

Search by name or AppId



All apps



DISPLAY NAME

APPLICATION TYPE

APPLICATION ID



Azure AD Domain Services Sync

Web app / API

c9816c72-abeb-4313-b495-ff76...

Microsoft Cloud Logging

- **Azure AD Logging** – Azure AD events – logons, user modification, password changes, administrator activity, etc.
- **Azure Security Center** – central console for security events and alerts for hybrid cloud (Azure/non-Azure).
- **Azure Log Analytics** - monitors cloud & on-prem availability and performance.
- **Cloud App Security** – Monitors logon and app activity.
- **Microsoft Operations Management Suite (OMS)** - Microsoft's cloud-based IT management solution.

Azure Log Analytics

defaultworkspace-f221fd98-0685-4071-aa19-537e10074aef-eus > Analytics

☺

📖

?

⚙️

Sean Metcalf

Home Page

+

↶

🏠

📁

📄

Export

⌵

🕒

Last 24 hours

⌵

▶

G

SCHEMA

FILTER

Filter by Name or Type

COLLAPSE ALL

ACTIVE

defaultworkspace-f221f... ☆

AntiMalware

LogManagement

Security

SecurityCenterFree

Updates

Functions

FAVORITES

Azure Log Analytics

Gain deep insights to your applications and systems.

SAVED QUERIES

FUNCTIONS

Members added To security-enabled groups [Category: Security Warning No...
SecurityEvent | where EventID in (4728, 4732, 4756) | summarize count() by Subjec...
On which machines and how many times have Windows Firewall Policy settin...
Event | where EventLog == "Microsoft-Windows-Windows Firewall With Advanced Secur...
Remote procedure call(RPC) attempts [Category: Security Info Notable Issues]
SecurityEvent | where EventID == 5712 | summarize count() by Computer
Security Activities on the computer "COMPUTER01.contoso.com" for account...
search in (SecurityEvent) Computer == "COMPUTER01.contoso.com" and TargetUserName...
Security Activities on the computer "Computer01.contoso.com" (replace with...
search in (SecurityEvent) Computer == "COMPUTER01.contoso.com" | project TimeGene...
Security groups created or modified [Category: Security Info Notable Issues]

COMMON QUERIES

DATA VOLUME

See the stream of data collected in the last 24 hour in intervals of 30 minutes

RUN

DATA TYPES

Show a distribution of your data by type over the last 24 hours

RUN

COMPUTERS

See which computers sent a heartbeat in the last hour and when they sent it

RUN

STALE COMPUTERS

Find out which computers haven't sent any data in the past 12 hours

RUN

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Default State: Microsoft Cloud Audit Logging

- No user or admin logging.
- No mailbox activity logging.

TL;DR: An organization's cloud admin has to enable logging before being able to properly monitor their environment.

Microsoft Cloud Security: What Really Matters



Limiting Access

- Overview
- Quick start
- MANAGE
- Users and groups
- Enterprise applications
- Devices (Preview)
- App registrations
- Application proxy
- Licenses
- Azure AD Connect
- Domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings**
- Properties
- Notifications settings

Save Discard

Enterprise applications

Users can consent to apps accessing company data on their behalf ⓘ

Yes No

Yes No

Users can add gallery apps to their Access Panel ⓘ

Yes No

Yes No

App registrations

Users can register applications ⓘ

Yes No

Yes No

External users

Guest users permissions are limited ⓘ

Yes No

Yes No

Admins and users in the guest inviter role can invite ⓘ

Yes No

Yes No

Members can invite ⓘ

Yes No

Yes No

Guests can invite ⓘ

Yes No

Yes No

Administration portal

Restrict access to Azure AD administration portal ⓘ

Yes No

Yes No

Azure AD Access Controls

- Admins and users in the guest inviter role can invite guests. [Yes]
- Guests can invite other guests (SharePoint sites or Azure resources). [No]
- Guest user permissions are limited (can't enumerate users, enumerate directory resources, or be member in admin roles). [Yes]
- Members can invite guests to collaborate (SharePoint sites or Azure resources). [No]
 - **No** means only administrators can invite guests.
- Restrict access to Azure AD administration portal.
 - **No** lets non-admins use the Azure AD administration portal to access AD resources user has permissions to read or manage resources they own.
 - Yes restricts all non-administrators from accessing any Azure AD data in admin portal. Doesn't restrict access other clients like PowerShell or Visual Studio.

Enable MFA

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for MFA. Before you begin, take a look at the [multi-factor auth deployment guide](#).

bulk update

View: Sign-in allowed users



Multi-Factor Auth sta

enable multi-factor auth

cancel

<input checked="" type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/>	John Arnold	JArnold@ingentech.co	Disabled
<input checked="" type="checkbox"/>	John Hammond	jhammond@ingentech.co	Disabled



About enabling multi-factor auth

Please read the [deployment guide](#) if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>

Enable MFA for all admins

```
$UserCredential = Get-Credential
Import-Module MSONline
Connect-MsolService -Credential $UserCredential

$auth = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement
$auth.RelyingParty = "*"

$auth.State = "Enabled"

$auth.RememberDevicesNotIssuedBefore = (Get-Date)

# Enable MFA on all Users
Get-MsolUser -All | where {$_.userprincipalname -like "*admin*"} | `
    Foreach {Set-MsolUser -UserPrincipalName $_.UserPrincipalName -StrongAuthenticationRequirements $auth }
```



Recommended for you

We recommend that you set passwords to never expire to avoid possible disruption. Currently, passwords expire every 730 days.

[View recommendation](#)

Office 365

Admin center

Sean Metcalf

Home

Users

Groups

Resources

Billing


Support

Settings

Setup

Reports

Change password settings



You're managing user accounts in the cloud, but haven't set your password expiration rule.

When your user accounts are managed in the cloud, we recommend that passwords are set to never expire. This will help users avoid the disruption of regular password changes. [Learn more about why we recommend this](#)

Set users passwords to never expire (recommended)

On

[Set a different password expiration rule](#)

Microsoft Password Guidance

Robyn Hicock, rhicock@microsoft.com

Microsoft Identity Protection Team

Purpose

This paper provides Microsoft's recommendations for password management based on current research and lessons from our own experience as one of the largest Identity Providers (IdPs) in the world. It covers recommendations for end users and identity administrators.

Microsoft sees over 10 million username/password pair attacks every day. This gives us a unique vantage point to understand the role of passwords in account takeover. The guidance in this paper is scoped to users of Microsoft's identity platforms (Azure Active Directory, Active Directory, and Microsoft account) though it generalizes to other platforms.

Summary of Recommendations

Advice to IT Administrators

Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

Administration:

Who has admin rights?

```
PS C:\> Get-MSOLRole | Format-Table ObjectId, Name

ObjectId                                     Name
-----
729827e3-9c14-49f7-bb1b-9608f156bbb8      Helpdesk Administrator
f023fd81-a637-4b56-95fd-791ac0226033      Service Support Administrator
b0f54661-2d74-4c50-afa3-1ec803f12efe      Billing Administrator
b5468a13-3945-4a40-b0b1-5d78c2676bbf      Mailbox Administrator
4ba39ca4-527c-499a-b93d-d9b492c50246      Partner Tier1 Support
e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8      Partner Tier2 Support
88d8e3e3-8f55-4a1e-953a-9b9898b8876b      Directory Readers
29232cdf-9323-42fd-ade2-1d097af3e4de      Exchange Service Administrator
75941009-915a-4869-abe7-691bfff18279e     Lync Service Administrator
fe930be7-5e62-47db-91af-98c3a49a38b1      User Account Administrator
9360feb5-f418-4baa-8175-e2a00bac4301      Directory Writers
62e90394-69f5-4237-9190-012177145e10      Company Administrator
d65e02d2-0214-4674-8e5d-766fb330e2c0      Email Verified User Creator
eb1d8c34-acf5-460d-8424-c1f1a6fbbdb85     AdHoc License Administrator
f28a1f50-f6e7-4571-818b-6a12f2af6b6c      SharePoint Service Administrator
d405c6df-0af8-4e3b-95e4-4d06e542189e      Device Users
9f06204d-73c1-4d4c-880a-6edb90606fd8      Device Administrators
9c094953-4995-41c8-84c8-3ebb9b32c93f      Device Join
c34f683f-4d5a-4403-affd-6615e00e3a7f      Workplace Device Join
17315797-102d-40b4-93e0-432062caca18      Compliance Administrator
d29b2b05-8046-44ba-8758-1e26182fcf32      Directory Synchronization Accounts
2b499bcd-da44-4968-8aec-78e1674fa64d      Device Managers
9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3      Application Administrator
cf1c38e5-3621-4004-a7cb-879624dced7c      Application Developer
5d6b6bb7-de71-4623-b4af-96380a352509      Security Reader
194ae4cb-b126-40b2-bd5b-6091b380977d      Security Administrator
e8611ab8-c189-46e8-94e1-60213ab1f814      Privileged Role Administrator
3a2c62db-5318-420d-8d74-23affee5d9d5      Intune Service Administrator
158c047a-c907-4556-b7ef-446551a6b5f7      Cloud Application Administrator
5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91      Customer LockBox Access Approver
44367163-eba1-44c3-98af-f5787879f96a      CRM Service Administrator
a9ea8996-122f-4c74-9520-8edcd192826c      Power BI Service Administrator
95e79109-95c0-4d8e-ae3-d01accf2d47b      Guest Inviter
b1be1c3e-b65d-4f19-8427-f6fa0d97feb9      Conditional Access Administrator
4a5d8f65-41da-4de4-8968-e035b65339cf      Reports Reader
```


Office 365 admin role	Translates to this in Exchange Online ...	Translates to this in SharePoint Online ...	Translates to this in Skype for Business Online.....	Translates to this in the Security & Compliance Center...
Global Admin	Exchange Online admin Company admin	SharePoint Online admin	Skype for Business admin	Security & Compliance Center admin (member of Organization Management role group)
Billing admin	N/A	N/A	N/A	N/A
Password admin	Help Desk admin*	N/A	Help desk admin	N/A
Service admin	N/A	N/A	N/A	N/A
User management admin	N/A	N/A	Skype for Business admin	N/A
Exchange administrator	Exchange Online admin	N/A	N/A	N/A
SharePoint administrator	N/A	SharePoint Online admin	N/A	N/A
Skype for Business administrator	N/A	N/A	Skype for Business admin	N/A
Compliance administrator	Organization Management	N/A	N/A	Compliance admin

```

import-module Msonline
$O365Roles = Get-MsolRole
ForEach ($O365RoleItem in $O365Roles)
{
    $RoleMembers = Get-MsolRoleMember -RoleObjectId $O365RoleItem.ObjectId
    IF ($RoleMembers)
    {
        Write-Output " $($O365RoleItem.Name): "
        $RoleMembers | Format-Table RoleMemberType,EmailAddress,DisplayName -AutoSize
    }
}

```

Directory Readers:

RoleMemberType	EmailAddress	DisplayName
ServicePrincipal		Microsoft.Azure.SyncFabric
ServicePrincipal		Azure AD Domain Services Sync

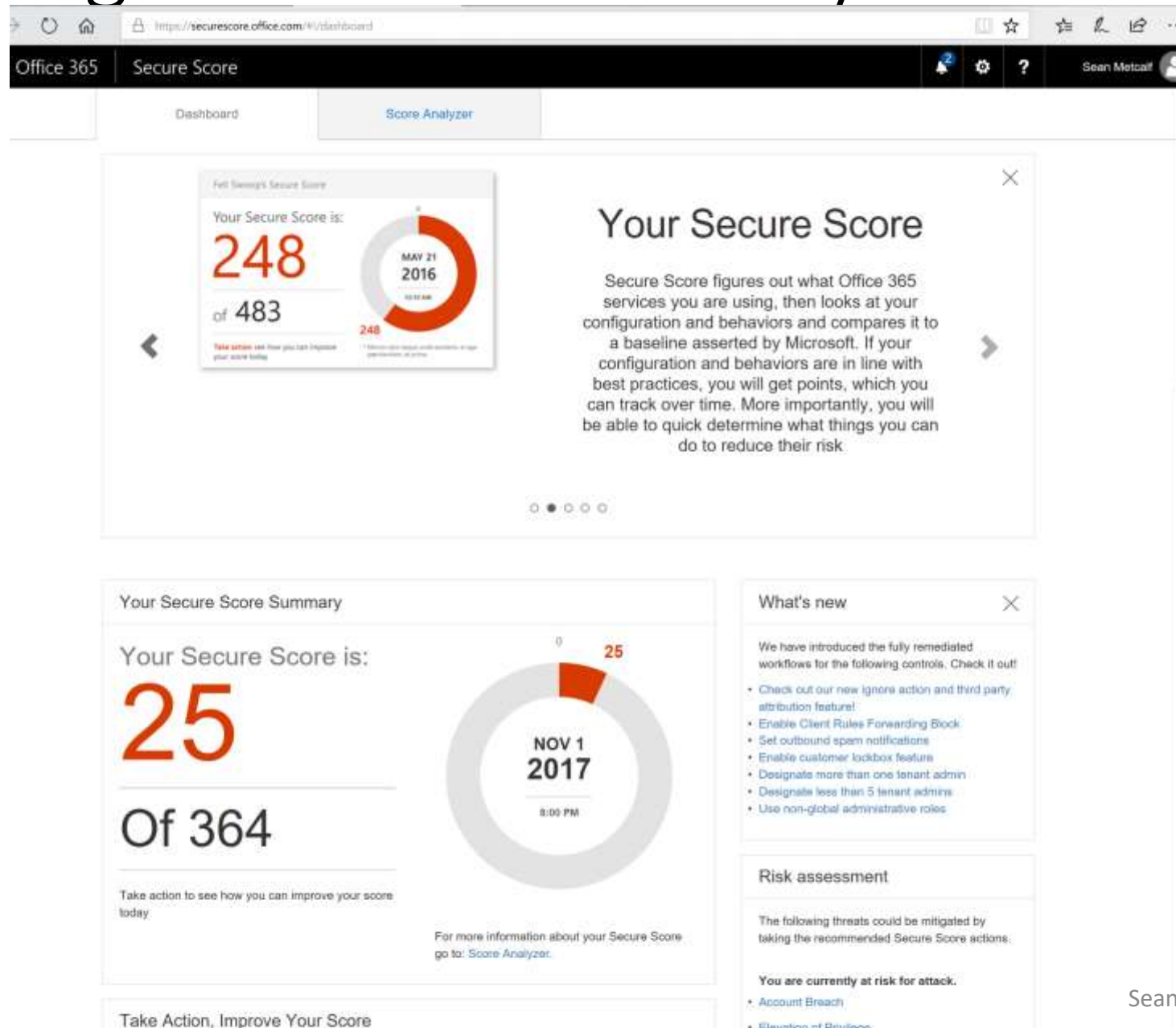
Company Administrator:

RoleMemberType	EmailAddress	DisplayName
User	sean@trimarcresearch.com	Sean Metcalf
User	JArnold@ingentech.co	John Arnold

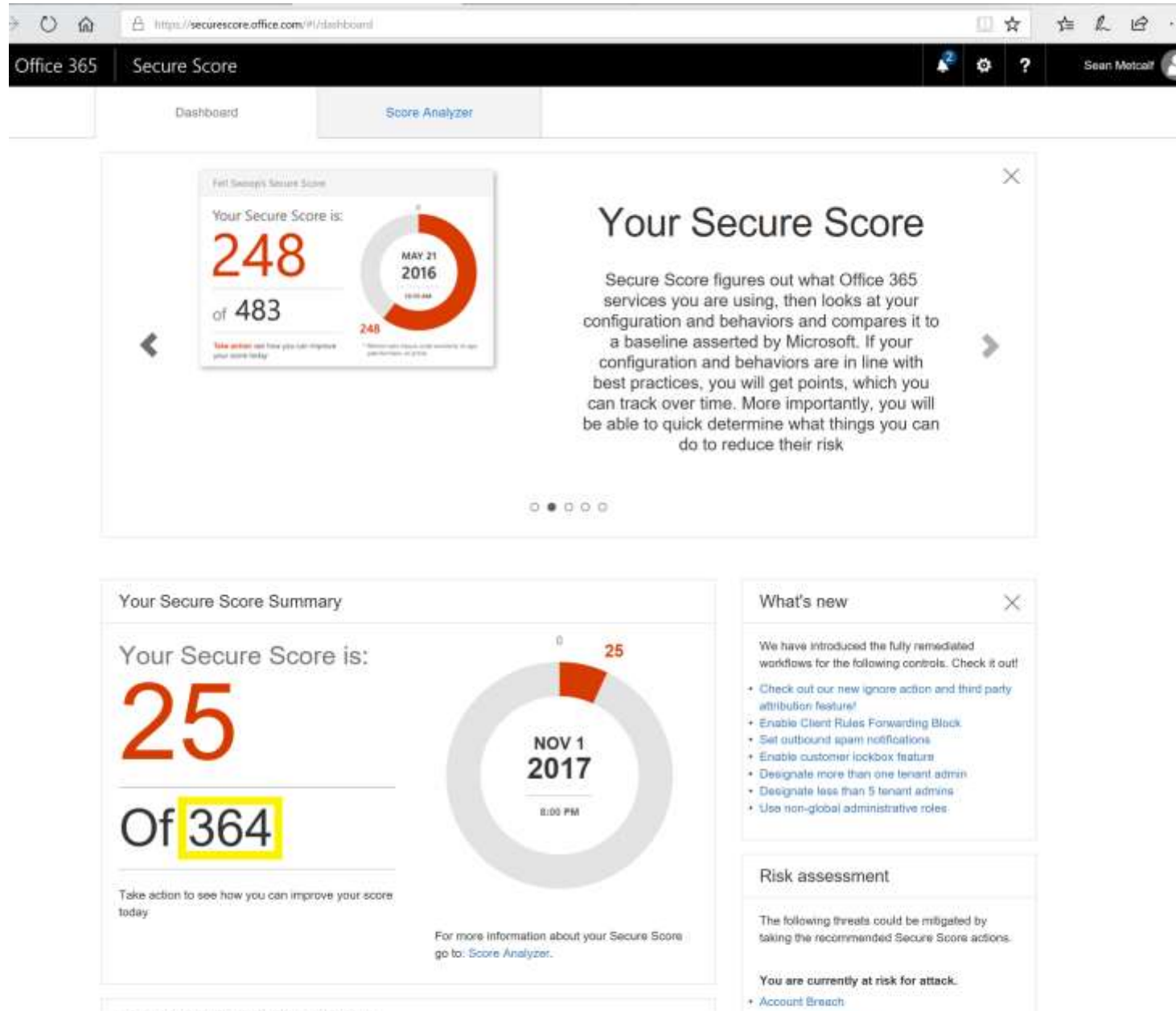
Email Verified User Creator:

RoleMemberType	EmailAddress	DisplayName
ServicePrincipal		Microsoft Office 365 Portal

Improving Office 365 Security: Secure Score



Improving Office 365 Security: Secure Score



27 Actions in the queue

Your pending Secure Score is: 316

Show:

All

[Expand all](#)

Enable MFA for all global admins



Enable MFA for all users



[Not Scored] Enable audit data recording

Enable Client Rules Forwarding Block
Advanced Action

Review signs-ins after multiple failures report weekly



[Not Scored] Set outbound spam notifications



Enable mailbox auditing for all users



Review sign-ins from unknown sources report weekly



Review signs-ins from multiple geographies report weekly



Review role changes weekly



Store user documents in OneDrive for Business



[Not Scored] Enable Information Rights Management (IRM) services



Use audit data

Sean Metcalf (@PyroTek3) TrimarcSecurity.com



27 Actions in the queue

Your pending Secure Score is: 316

Category		Expand all ▾
Show	All	
	Account	
	Data	
Enable	Device	ns ▾
Action Type		
	Behavior	
Enable	Configuration	▾
	Review	
User Impact		
[Not	Low	recording ▾
	Moderate	
Implementation Cost		
Enable	Low	g Block ▾
Adv	Moderate	
Control Type		
	Advanced	
Rev	Standard	failures report weekly ▾
[Not Scored] Set outbound spam notifications		▾
Enable mailbox auditing for all users		▾

What am I about to change?

There are several ways today that a bad actor can use external mail forwarding to exfiltrate data.

1. Client created external mail forwarding Rules, such as the Outlook desktop client.
2. Admins can set up external mail forwarding for a user via setting ForwardingSmtpAddress on a user object.
3. Admins can create external transport rules to forward messages.
4. Client created ForwardingSmtpAddress via Outlook Web Access interface

Enable Client Rules Forwarding Block Complete

This Security Control action will help mitigate Client created external mail forwarding rules.

You have successfully created the transport rule that blocks the use of client-side forwarding rules.
Your score will increase by 20 points within 24 hours.

A simple mitigation is to, on each Remote Domain, including the Default to disallow Auto-Forwarding. This is a global setting and applies to every email sent from within a Tenant, as a result it is a very broad approach, which does not allow white listing. More details can be found [here](#). RBAC roles can be used to achieve a similar result.

Using a properly configured Transport Rule we can control the impact of data exfiltration via Client created external mail forwarding rules. This approach has a couple of advantages:

1. Clients will receive a custom NDR message, useful for highlighting to end users external forwarding rules they may have not known existed (accidental exfiltration), or external forwarding rules created by a bad actor on a compromised mailbox.
2. Allows a whitelist of users or groups to be configured to allow business approved exceptions to the policy.
3. Provides some mitigation, for when an Admin account has been used to create a Remote Domain with auto-forwarding enabled to specific namespace to exfiltrate data.
4. Provides some mitigation, for when an Admin account has been used to alter the Default Remote Domain settings.

This Security Control will create a transport rule that will stop external messages leaving your Tenant, that are of the type AutoForward, mitigating the use of Client created external mail forwarding rules and malicious Remote Domain entries as a data exfiltration vector.

1. If The Sender is located 'Inside the organization'
2. If The Recipient is located 'Outside the organization'
3. If The message type is 'Auto-Forward'

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Apply

More ⇄

Cancel

Enable mailbox auditing for all users

You should enable mailbox auditing for at least ninety percent of all users that have mailboxes in your tenancy. By default all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user's account has been breached. We found that you had 0 mailboxes of 6 with audited enabled. If you enable mailbox auditing on at least ninety percent of your mailboxes, your score will go up 10 points.

Action Category

Data

User Impact

Low

Implementation Cost

Low

Action Score

0/10

Threats

- [Account Breach](#)

[Learn more](#)[Ignore](#)[Third Party](#)

Azure Security Center

*”Azure Security Center **provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds. It delivers visibility and control over hybrid cloud workloads, active defenses that reduce your exposure to threats, and intelligent detection to help you keep pace with rapidly evolving cyberattacks.***

*The Security Center Overview provides a quick view into the security posture of your Azure and non-Azure workloads, enabling you to **discover and assess the security of your workloads and to identify and mitigate risk.***”

Search (Ctrl+F)

GENERAL

Overview

Security policy

Quickstart

Welcome

Events

Onboarding to advanced sec...

Search

PREVENTION

Recommendations

Security solutions

Compute

Networking

Storage & data

Applications

Identity & Access

DETECTION

Security alerts

Custom alert rules (Preview)

Threat intelligence

Power BI Subscriptions Log Integration

Overview

Recommendations

4 Total

Security solutions

1 Total

New alerts & incidents

0 0

Events - last week

4.7K Total

Prevention

Compute

1 Total

Networking

0 Total

Storage & data

3 Total

Applications

0 Total

Detection

Security alerts

No security alerts

Most attacked resources

No attacked resources to display

Advanced cloud defense

Just in time VM access - last week (Preview)

PROTECTED
0 VMs
APPROVED REQUESTS
0 Total

31 Dec

Adaptive application controls (Preview)

0 Adaptive applications control is now in public preview. Please follow the link to learn more and register.
[Enable Application Whitelisting](#)

Azure Security Center

- Free Tier:
 - basic security policy, security recommendations, and integration with security products and services from partners.
- Standard Tier: \$15/node/month
 - Hybrid security
 - Advanced threat detection
 - Whitelisting controls
 - Just in Time access to Azure VMs
 - Free for 60 days
- Configurable Security Policies
- Microsoft monitoring agent (port 443) leverages ETW and event log data
- Recommendations provide actions
- Integration from other elements (ex. Azure AD Identity Protection)

Enable Azure Security Center

 Upgrade to the Standard tier for enhanced security

Protect your hybrid cloud workloads with unified security and threat management


Hybrid security


Advanced threat detection


JIT VM access


Adaptive application controls


Upgrade the following subscriptions and workspaces to enable Security Center Standard:

<input checked="" type="checkbox"/>	NAME	RESOURCES	CURRENT PRICING TIER	
<input checked="" type="checkbox"/>	 Pay-As-You-Go	0 applicable resources	Free	Upgrade >
<input checked="" type="checkbox"/>	 Pay-As-You-Go	0 applicable resources	Free	Upgrade >
<input checked="" type="checkbox"/>	 Pay-As-You-Go	0 applicable resources	Free	Upgrade >
<input checked="" type="checkbox"/>	 Pay-As-You-Go	0 applicable resources	Free	Upgrade >

Apply Standard plan
First 60 days are free!

Security Center Highlights Potential Issues

Security Center - Recommendations

 Search (Ctrl+/)

GENERAL



Overview



Security policy



Quickstart



Welcome



Events



Onboarding to advanced sec...







Search

PREVENTION



Recommendations

 Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Endpoint Protection not installed on Azure VMs	InGenAdmin1	Open	 High	...
Apply a Just-In-Time network access control (preview)	InGenAdmin1	Open	 High	...
Apply disk encryption	InGenAdmin1	Open	 High	...
Provide security contact details	1 subscriptions	Open	 Medium	...

Connect Additional Data Sources for Better Insight

Security Center - Security solutions

Search (Ctrl+/)

GENERAL

- Overview
- Security policy
- Quickstart
- Welcome
- Events
- Onboarding to advanced sec...
- Search

PREVENTION

- Recommendations
- Security solutions**
- Compute
- Networking
- Storage & data
- Applications
- Identity & Access

Filter

Connected solutions (1)

View all security solutions currently connected to Azure Security Center, monitor the health of solutions, and access the solutions' management tools for advanced configuration.

Identity protection
MICROSOFT
Azure AD Identity Protection
Connected
[VIEW](#)

Add data sources (3)

Connect your security solution to Azure Security Center.

Non-Azure computers
MICROSOFT
Onboard your non-Azure computers to Azure Security Center and gain security assessment, recommendations and more powerful features
[ADD](#)

Common Event Format
ANY PUBLISHER
Integrate any security solution that support Common Event Format (CEF), take advantage of Search & Custom Alert Rules, and Threat Intelligence enrichment for each log
[ADD](#)

Advanced Threat Analytics
MICROSOFT
Integrate Microsoft Advanced Threat Analytics suspicious activities along with other detections in your environment, and gain correlations and otherwise undetectable
[ADD](#)

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Adaptive Application Controls

Security Center - Adaptive application controls (Preview)

Search (Ctrl+/)

Recommendations

Security solutions

Compute

Networking

Storage & data

Applications

Identity & Access

DETECTION

Security alerts

Custom alert rules (Preview)

Threat intelligence

ADVANCED CLOUD DEFENSE

Adaptive application control...

Just in time VM access (Previ...

AUTOMATION & ORCHESTRATION

Playbooks (Preview)

What is application control?

Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs

How does it work?

Security Center analyzes data of processes to find VMs for which there is a constant set of running applications. Security Center creates whitelisting rules for each resource group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

[For more information go to the documentation>](#)

Here's a sample of the information you'll be getting once you've enabled **Application whitelisting**

Relevant processes that run on your VMs and we recommend you to whitelist:

NAME	VMs	PROCESSES
Subscription 1	3	7
C:\ProgramFiles\		
C:\ProgramFiles\Octopus Deploy\Tentacle\Te...		
C:\Octopus\Calamari\3.3.13\Octodiff.exe		
C:\ProgramFiles\Octopus Deploy\Tentacle\Te...		
C:\Octopus\Calamari\3.3.13\Octodiff.exe		
C:\Octopus\Calamari\3.3.13\Octodiff.exe		
C:\ProgramFiles\Octopus Deploy\Tentacle\Te...		
C:\Octopus\Calamari\3.3.13\Octodiff.exe		

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Time: Last 24 hours

IDENTITY POSTURE

Logons



Accounts logged on

2 ↗ 2

Accounts failed to log on

114 ↗ 82

Locked accounts

0

Accounts with changed or reset password

0

Active critical notable issues

0

Active warning notable issues

0

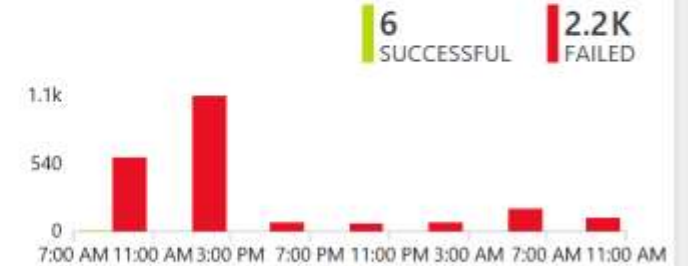
FAILED LOGONS

Failed logon reasons



ACCOUNT	FAILED ↓	ATTEMPTS
administrator	100%	372
adm	100%	89
test	100%	81
admin	100%	76
scan	100%	73
user	100%	72
backup	100%	71
test2	100%	71
temp	100%	71
scans	100%	71
See all...		

LOGONS OVER TIME

[See all...](#)

Time: Last 24 hours

IDENTITY POSTURE

Logons



Accounts logged on

2 ↗ 2

Accounts failed to log on

114 ↗ 82

Locked accounts

0

Accounts with changed or reset password

0

Active critical notable issues

0

Active warning notable issues

0

FAILED LOGONS

Failed logon reasons



ACCOUNT

FAILED



ATTEMPTS

administrator 100% 372

adm 100% 89

test 100% 81

admin 100% 76

scan 100% 73

user 100% 72

backup 100% 71

test2 100% 71

temp 100% 71

scans 100% 71

[See all...](#)

LOGONS OVER TIME

[See all...](#)

Just In Time (JIT) VM Access Configuration

JIT VM access configuration

InGenAdmin1 - PREVIEW

+

Add

Save

×

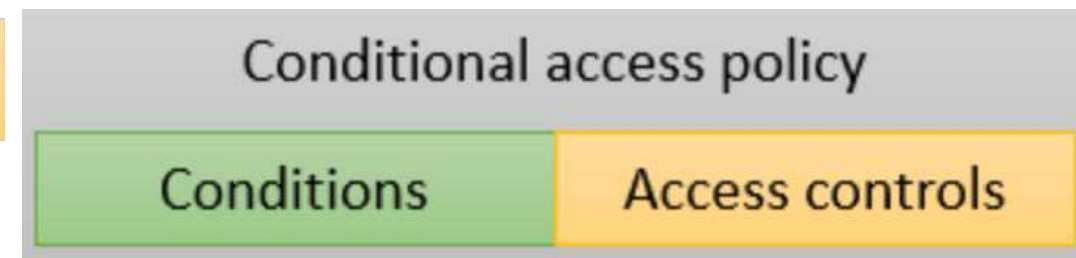
Discard

Configure the ports for which the just in time VM access will be applicable.

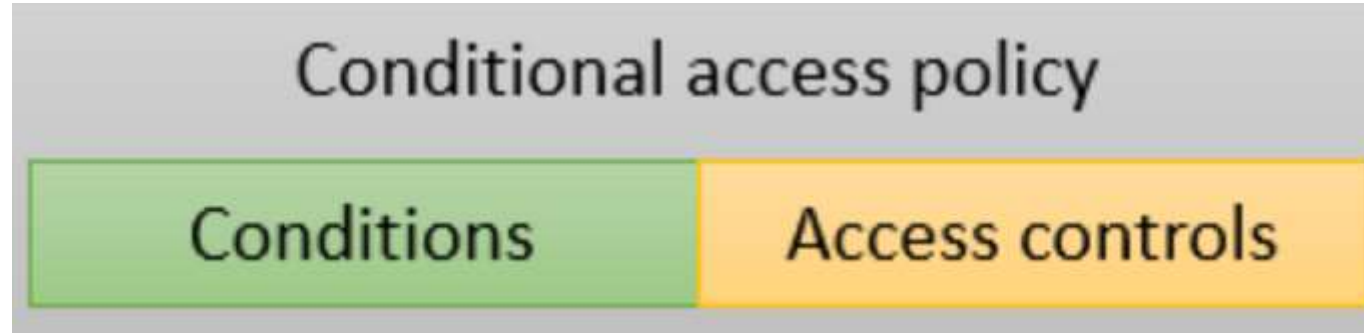
PORT	PROT...	ALLOWED SOUR...	IP RANGE	TIME RANGE	
22 <i>(Recommended)</i>	Any	Per request	N/A	3 hours	...
3389 <i>(Recommended)</i>	Any	Per request	N/A	3 hours	...
5985 <i>(Recommended)</i>	Any	Per request	N/A	3 hours	...
5986 <i>(Recommended)</i>	Any	Per request	N/A	3 hours	...

Azure AD Conditional Access

- Enforce different rules on authentication/access based on a variety of conditions.
- Control access based on:
 - Sign-in activity (anomalies?)
 - Network location (corporate network vs internet)
 - Device (registered with Azure or not)
 - Application (Outlook vs OWA vs EWS)
- Requires Azure AD P1



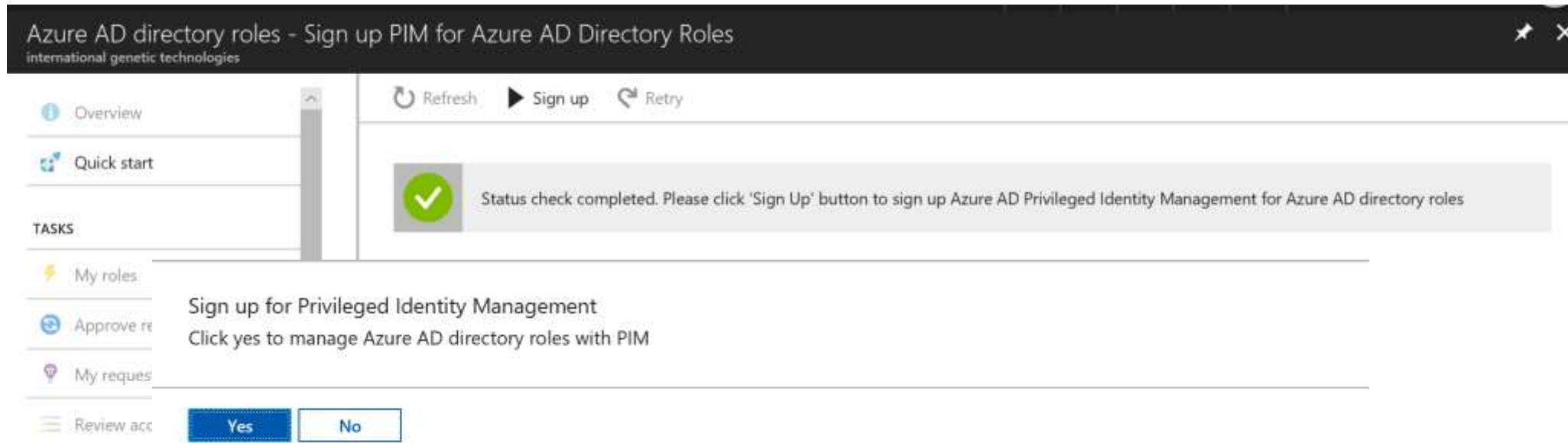
Azure AD Conditional Access



- Enforce different rules on authentication based on user location (on-prem vs. internet).
- Control access based on:
 - Sign-in activity
 - Network location
 - Device
 - Application

Azure AD Privileged Identity Management (Preview)

- Removes permanent admin access & better track who has what rights when.
- Enables “just in time” admin rights based on role.
- Provides approval workflow (auto-approved or single approver from list).
- Access expires automatically once the threshold is reached after approval.

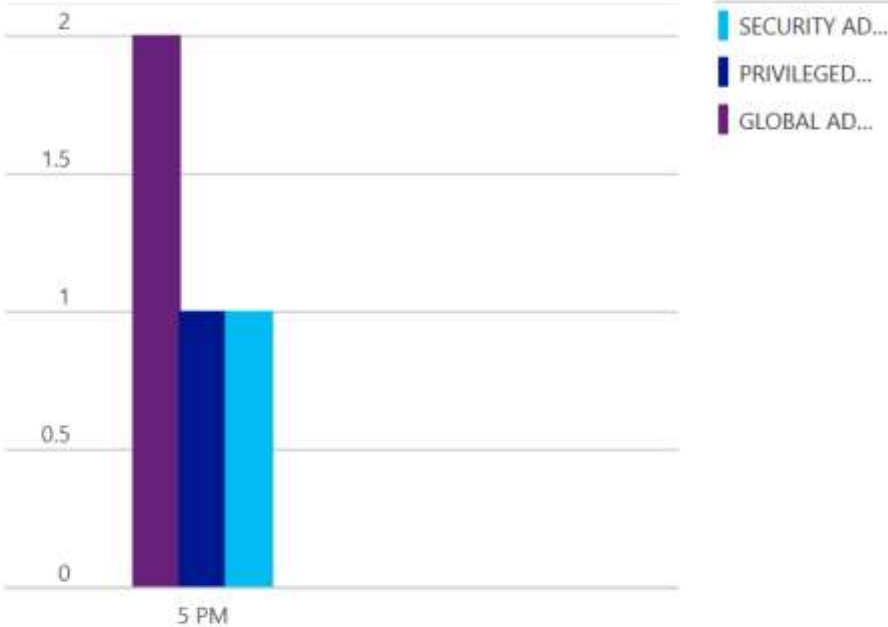


- Overview
- Quick start
- TASKS
- My roles
- Approve requests (preview)
- My requests (preview)
- Review access
- MANAGE
- Roles
- Users
- Alerts
- Access reviews
- Wizard
- Settings
- Sign up PIM for Azure AD Dir...

Refresh

Admin viewMy view

My Activation history for the past 7 days



DIRECTORY ACTIVATION...

4

Approve requests

ApproveDenyRefresh

REQUESTORROLEREASONREQUEST RECEI...

My roles

Eligible role assignments

ROLE NAME	STATUS	ACTION
No roles found		

Active role assignments

ROLE NAME	STATUS	ACTION
Security Administrator	Permanently assigned	
Global Administrator	Permanently assigned	
Privileged Role Admin	Permanently assigned	

 Save  Discard

Activations

Maximum activation duration (hours) ⓘ

 1

Notifications

Send email notifying admins of activation ⓘ

Enable Disable

Require approval

Require approval to activate this role ⓘ

Enable Disable

Incident/Request ticket

Require incident/request ticket number during activation ⓘ

Enable **Disable**



Self-approval is not allowed, we recommend to add at least 2 approvers.

SELECTED APPROVER

ACTION



John Hammond
jhammond@ingentech.co

Remove

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation ⓘ

Enable Disable

Select approvers

Add more approvers

My Azure AD directory roles

Refresh

Eligible role assignments

ROLE NAME	STATUS	ACTION
 Global Administrator	Request activation	

Active role assignments

ROLE NAME	STATUS	ACTION
-----------	--------	--------

No roles found

Global Administrator

Role activation details

▶ Activate

■ Deactivate

Name

John Arnold

Email

JArnold@ingentech.co

Activation

Eligible

Expiration

Request role activation

Global Administrator

* Reason for role activation ⓘ

Need to update global settings as per Hammond.

✓

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

Azure Active Directory

Privileged role activation pending approval

JArnold@ingentech.co trying to activate to Company Administrator role in TrimarcResearch.onmicrosoft.com


Azure Active Directory Privileged Identity Management allows organization to enable just in time administrator access and administrator access based on approval. You have been configured as one of the approvers for Company Administrator in Azure Active Directory TrimarcResearch.onmicrosoft.com.

JArnold@ingentech.co requested activation to Company Administrator role, with the following activation reason: Need to update global settings as per Hammond.

Please [follow the link](#) to approve or deny the request.

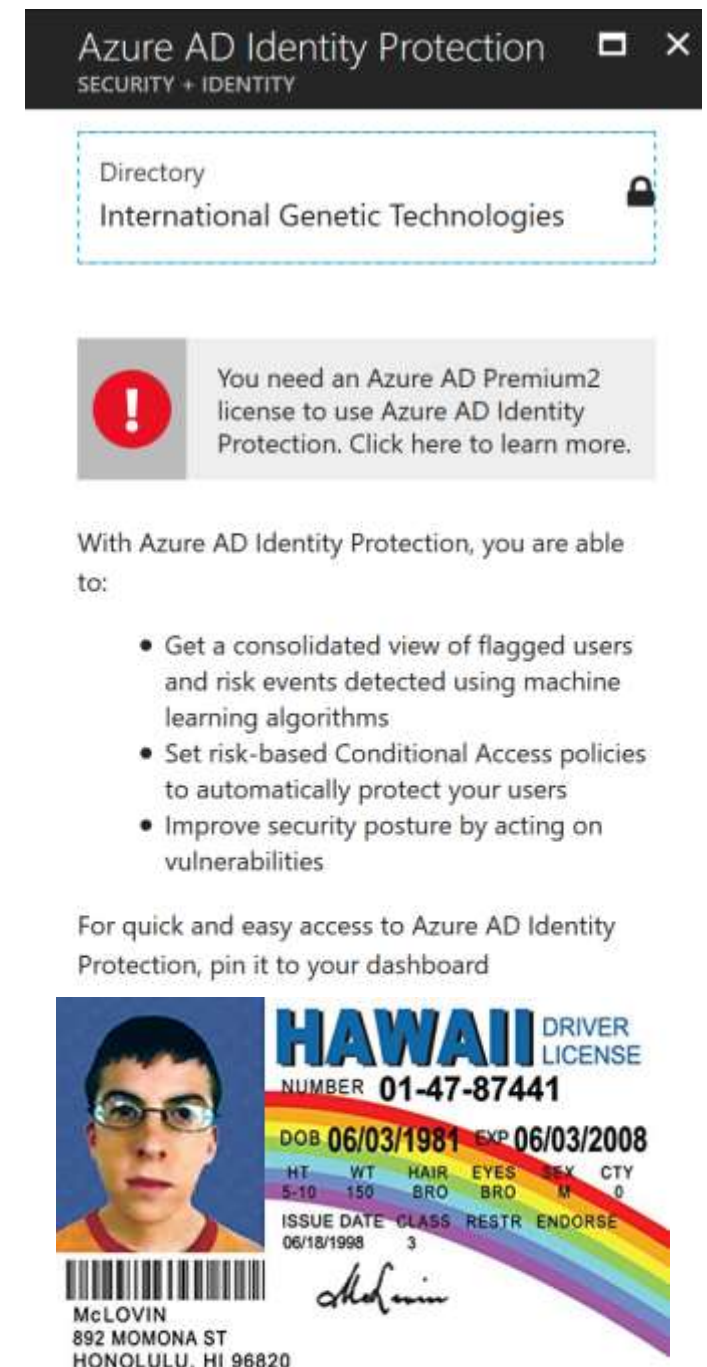
Directory roles - Approve requests (preview)
Technologies

✓ Approve ✕ Deny ↺ Refresh

REQUESTOR		ROLE	REASON	REQUEST RECEIVED
<input checked="" type="checkbox"/>	 John Arnold JArnold@ingentech.co	Global Administrator	Company info update.	Sat Nov 04 2017 18:13:41...

Azure AD Identity Protection

- Requires Azure AD Premium (P2)
- Configure automated responses to detected suspicious actions that are related to your organization's identities
- Investigate suspicious incidents and take appropriate action to resolve them
- Configure risk-based policies that respond to detected issues at a specified risk level.
- Policies can either block or initiate adaptive remediation actions including password resets & MFA enforcement.



Azure AD Identity Protection
SECURITY + IDENTITY

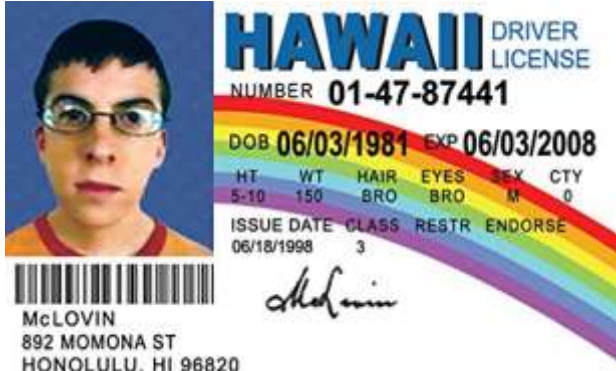
Directory
International Genetic Technologies

! You need an Azure AD Premium2 license to use Azure AD Identity Protection. [Click here to learn more.](#)

With Azure AD Identity Protection, you are able to:

- Get a consolidated view of flagged users and risk events detected using machine learning algorithms
- Set risk-based Conditional Access policies to automatically protect your users
- Improve security posture by acting on vulnerabilities

For quick and easy access to Azure AD Identity Protection, pin it to your dashboard



HAWAII DRIVER LICENSE
NUMBER 01-47-87441
DOB 06/03/1981 EXP 06/03/2008
HT 5-10 WT 150 HAIR BRO EYES BRO SEX M CTY 0
ISSUE DATE 06/18/1998 CLASS 3 RESTR ENDORSE
McLOVIN
892 MOMONA ST
HONOLULU, HI 96820

GENERAL

Overview

Getting started

INVESTIGATE

Users flagged for risk

Risk events

Vulnerabilities

CONFIGURE

Multi-factor authentication regi...

User risk policy

Sign-in risk policy

SETTINGS

Alerts

Weekly Digest

Pin to dashboard

Refresh

Identify users who are assigned to permanent admin role →

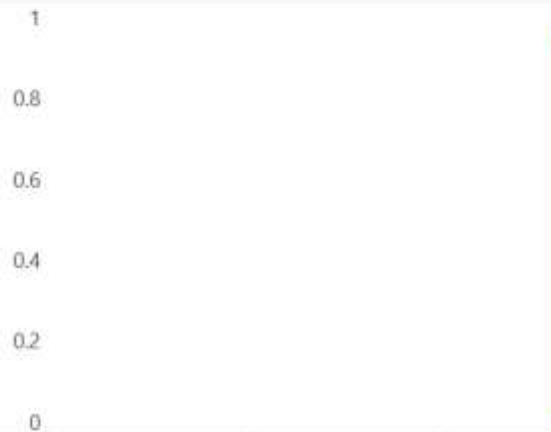
Users flagged for risk



AT R...
1

SEC...
0

Risk events



08/07 09/06 10/06
HIGH 0 MEDIUM 1 LOW 0 CLOSED 0

Vulnerabilities ⓘ

1

RISK LEVEL	COUNT	VULNERABILITY
Medium	2	Users without multi-factor authentication registration

Integrate Azure AD Identity Protection

Azure Active Directory Identity Protection provides a consolidated view of at risk users and vulnerabilities, with the ability to remediate risk immediately, and set policies to remediate future events.

The service is built on Microsoft's experience protecting consumer identities, and provides tremendous accuracy from the signal from over 13B logins a day.

With Azure AD Identity Protection, you can:

Integrate Microsoft Azure AD Identity Protection alerts along with other detections in your environment and gain correlations and otherwise undetectable attacks by combining low fidelity detections across all your security data.

Get identity data from multiple sources and view all user anomalies and alerts in one place that surfaces all users realted information so you can easily understand how risky each user is.

When using the Azure AD Identity Protection, you can get all

- Leaked credentials
- Impossible travel to atypical locations
- Sign-ins from anonymous IP addresses
- Sign-ins from IP addresses with suspicious activity

Cloud App Security

- Discover cloud app use - sanction and unsanction apps [Azure AD P1]
- Enforce DLP policies and configure alerting
- Detect anomalous use and security incidents.



Create new Cloud Discovery snapshot report

Fill in the following details and upload recent traffic logs from your organization to create a new report.

[Privacy statement](#)

Report name

Description

Data source

☐ Anonymize private information

Store and display only encrypted usernames.

Choose traffic logs

1 GB maximum size per log, from the last 90 days

Report creation process

⌚ Analysis takes up to 24 hours | [Track status](#)

- Upload
- Parse
- Data analysis
- Generate report



[View sample report](#)



General dashboard

View dashboard for a specific app

- Microsoft Office Online
- Microsoft Power BI
- Microsoft Teams
- Yammer
- Microsoft OneDrive for Business
- Microsoft SharePoint Online
- Microsoft Exchange Online
- Office 365

[View all apps...](#)

View dashboard for a specific risk type

- Threat detection
- Privileged accounts
- Compliance
- DLP
- Cloud Discovery
- Sharing control
- Access control
- Configuration control

General dashboard

460 activities monitored

10 files monitored

4 accounts monitored

Discover your cloud apps
upload traffic logs

0 governance actions taken

0 user notifications sent

15 Open alerts
New over the last month

RECENT ALERTS

- All Admin Activity** 22 minutes ago
sean@trimarcresearch.com
Microsoft Cloud App Security
- All Admin Activity** 11 hours ago
sean@trimarcresearch.com
Office 365
- All Admin Activity** 16 hours ago
sean@trimarcresearch.com
Office 365

[View all alerts in the last month...](#)

BY SEVERITY



BY ALERT TYPE



Top 3 alert types

- 15 Activity policy alert
- N/A
- N/A

37 Activity violations
New over the last month

0 Content violations
New over the last month

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

37 All Admin Activity



Activity log

APP

USER NAME

RAW IP ADDRESS

ACTIVITY TYPE

LOCATION

Advanced

Select apps... ▾

Select users... ▾

Select activity... ▾

Select countries/regions... ▾

1 - 20 of 460 activities ⓘ

New policy from search



Activity	User	App	IP address	Location	Device	Date ▾	
Log on	sean	Microsoft...	70.21	United Sta		Nov 6, 2017, ...	⋮
Set company information: proper	sean	Office 365	N/A	—	Other	Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Office 365	70.21	United Sta		Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Office 365	70.21	United Sta		Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Office 365	70.21	United Sta		Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Office 365	70.21	United Sta		Nov 6, 2017, ...	⋮
Set company information: proper	sean	Office 365	N/A	—	Other	Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Microsoft...	70.2	United Sta		Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Office 365	70.2	United Sta		Nov 6, 2017, ...	⋮
Log on	Sean Metcalf	Office 365	70.2	United Sta		Nov 6, 2017, ...	⋮

Create activity policy

Policy template

No template *

Policy name

All Admin Activity

Description

Policy severity

Low *

Category

Privileged accounts *

Create filters for the policy

Act on:

- ☒ Single activity
Every activity that matches the filters
- ☐ Repeated activity:
Repeated activity by a single user

ACTIVITIES MATCHING ALL OF THE FOLLOWING [Edit and preview results](#)

is

[+](#)

Alerts

☒ Create alert [Use your organization's default settings](#)

Daily alert limit

☐ Send alert as email ⓘ

☐ Send alert as text message ⓘ

[Save these alert settings as the default for your organization](#)

Governance

>  All apps

>  Office 365

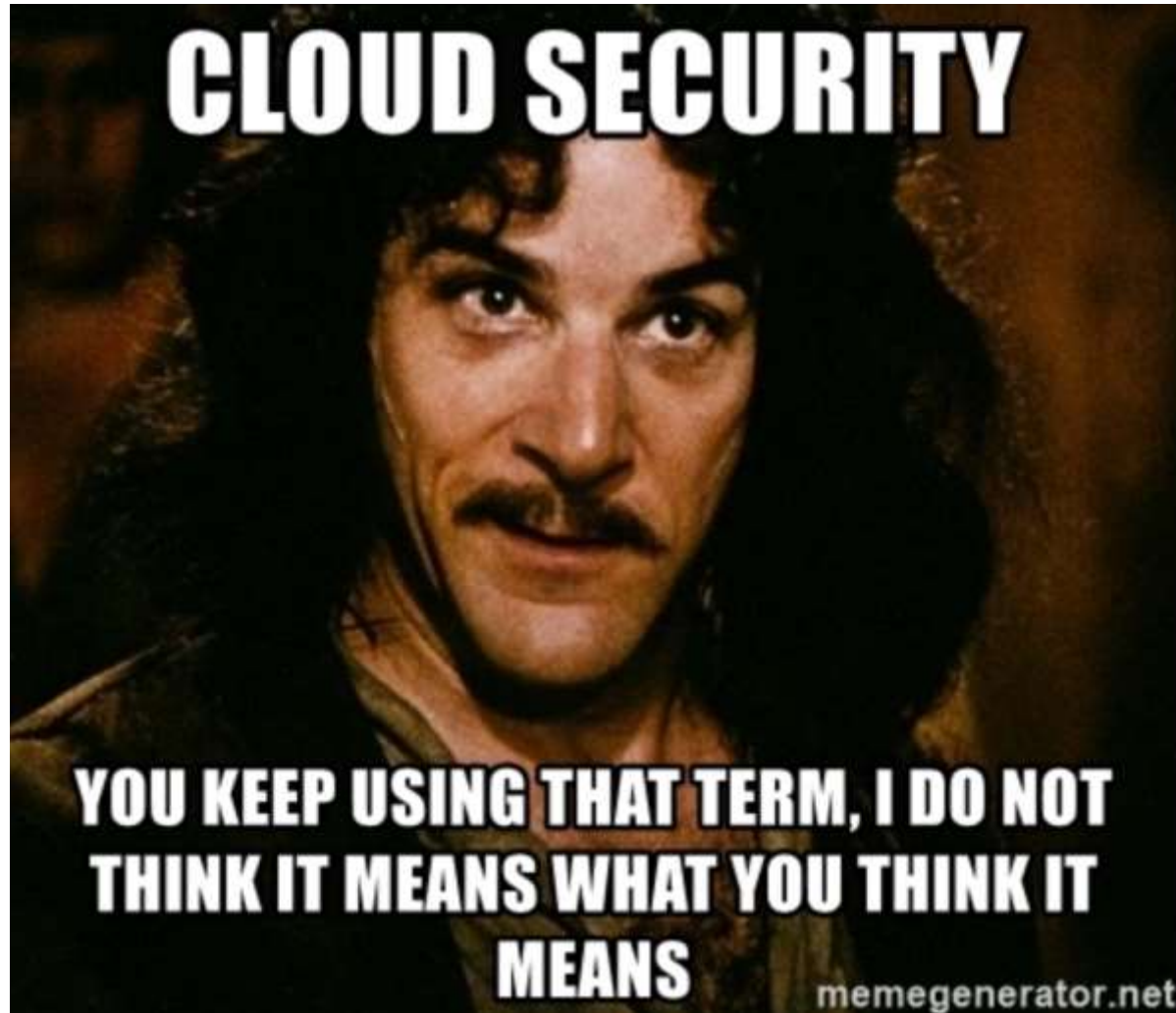
Security Center, Cloud Security, & Secure Score, Oh My!

- (Azure) Security Center
 - Effectively a Cloud SIEM with threat intel and controls.
- (Office 365) Cloud Security App
 - Cloud app usage discovery and app data control.
- (Office 365) Secure Score
 - Recommended Office 365 security configuration checks and implementation guidance.
- (Azure AD) Conditional Access [Azure AD P1]
 - Control access and authentication types.
- (Azure AD) Privileged Identity Management [Azure AD P2]
 - Approval workflow and management of admin roles.
- (Azure AD) Identity Protection [Azure AD P2]
 - Manage and limit risk of identity loss.

Azure AD Tiers

- Free
 - Dynamically banned passwords (prevents user from setting really bad passwords).
- Basic: \$1 per user monthly
 - No object limit
 - Basic reports
- P1: \$6 per user monthly
 - Self-Service Group and app Management
 - Self Service Password Reset
 - Two-way sync between on-prem & Azure AD
 - Cloud App Discovery
 - Conditional Access based on group, location, and device state
 - MDM auto-enrollment
- P2: \$9 per user monthly
 - Includes P1 features
 - Identity Protection
 - Privileged Identity Management

Cloud Security Best Practices



Cloud Recommendations Summary

- Consider removing DNS txt records created to on-board cloud services.
- Discover accounts in AD that may be synchronizing on-prem AD with a cloud service.
- Ensure Azure AD Connect doesn't have rights it doesn't need.
- Disable user access protocols that aren't required - goal is Modern Auth with MFA.
- Protect Azure AD Connect & federation servers like DCs.
- Protect cloud admins like AD admins.
- Ensure on-prem admin accounts are not cloud enabled.
- Ensure only Domain Admins has permissions on highly privileged service accounts.
- Enable user and admin activity logging in Office 365 (UnifiedAuditLogIngestionEnabled).
- Limit who has Global Admin rights.
- Enable mailbox activity auditing on all O365 mailboxes.
- Monitor App registrations.
- Limit user access to Azure AD.
- Enable MFA on all accounts, especially admin accounts.
- Review the recommendations in Office Secure Score and implement as many as possible.


VM Recommendations

- Rename the local Administrator account & change the password.
- Limit management protocol access (JIT).
- Azure Security Center can monitor alerts.

FAILED LOGONS

Failed logon reasons



ACCOUNT	FAILED 	ATTEMPTS
administrator	100%	237
test	100%	182
admin	100%	178
user1	100%	176
scan	100%	176
temp	100%	176
scans	100%	176
reception	100%	175
testuser	100%	175
test1	100%	175
See all...		

Protecting Admin Accounts

- Enforce MFA on all admin accounts
- Many of the basics remain the same
 - Least privilege is key and poorly understood in many cloud implementations
 - Least access, use the security features provided by the cloud
 - Cloud admin workstations – treat same as privileged users
- Limit admin role membership and monitor group membership. PIM can help.

Monitoring and alerting

- It's not just for your network any more
- Defenders need to work with DevOps to make sure that cloud resources and data are considered in defensive designs
- Different cloud providers provide different tools for managing security
- Defenders must be familiar with the tools from cloud providers.
- Log collection and management needs to include cloud assets
- You do know what your assets are, right?
- Assume breach!

Summary

- Cloud is a new paradigm requiring careful planning.
- Securing cloud resources isn't straight forward.
- Many items that apply to on-premises also applies to cloud.



Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

References

Azure AD

<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-what-is>

Azure AD Connect

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect>

Azure AD Domain Services

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

Amazon AWS Directory FAQ

<https://aws.amazon.com/directoryservice/faqs/>

Azure Security Center

<https://docs.microsoft.com/en-us/azure/security-center/security-center-intro>

Cloud App Security

<https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security>

References

Azure Network Security Best Practices

<https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices>

Azure security best practices and patterns

<https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns>

Azure virtual machine security best practices

<https://docs.microsoft.com/en-us/azure/security/azure-security-best-practices-vm>

Azure identity & access security best practices

<https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices>

Security Best Practices for Windows Azure Solutions - Download Center

<http://download.microsoft.com/download/7/8/a/78ab795a-8a5b-48b0-9422-fddee8f70c1/securitybestpracticesforwindowsazuresolutinsfeb2014.docx>

References

Amazon AWS PowerShell

<https://aws.amazon.com/powershell/>

Google Cloud PowerShell

<https://cloud.google.com/powershell/>

Microsoft Azure PowerShell

<https://docs.microsoft.com/en-us/powershell/azure/install-azurermps?view=azurermps-4.1.0>

Microsoft Office 365 PowerShell

<https://technet.microsoft.com/en-us/library/dn975125.aspx>

References

OWA-Toolkit

<https://github.com/johnnyDEP/OWA-Toolkit>

MailSniper: Invoke-PasswordSprayOWA

<https://github.com/dafthack/MailSniper>

Patator:

<https://github.com/lanjelot/patator>

LyncSniper: <https://github.com/mdsecresearch/LyncSniper>

<https://www.mdsec.co.uk/2017/04/penetration-testing-skype-for-business-exploiting-the-missing-lync/>

Detectify - AWS S3 Misconfigurations Explained

<https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/>

Infiltrate 2017: Cloud Post Exploitation Techniques - Andrew Johnson & Sacha Faust

<https://vimeo.com/214855977>

References

The AWS Security Best Practices white paper

https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

The EC2 Instances Best Practices white paper

<https://aws.amazon.com/articles/1233/>

Finding API keys

<https://hackernoon.com/how-to-use-environment-variables-keep-your-secret-keys-safe-secure-8b1a7877d69c>

AWS Credential Management






<https://github.com/awslabs/git-secrets>

AWS re:Invent 2016: Automating Security Event Response, from Idea to Code to Execution

<https://www.youtube.com/watch?v=x4GkAGe65vE>

0365 SharePoint Controls

SharePoint Data Access Controls

 Office 365 | Admin    Sean Metcalf 

SharePoint admin center

site collections

infopath

user profiles

bcs

term store

records management

search

secure store

apps

sharing

settings

configure hybrid

access control

Restrict access based on device or network location

These settings apply to content in SharePoint, OneDrive, and Office 365 groups.

Unmanaged devices

Control access from devices that aren't compliant or joined to a domain. The setting you select here will apply to all users in your organization. To customize conditional access policies, save your selection and go to the [Azure AD admin center](#).

☒ Allow full access from desktop apps, mobile apps, and the web

☐ Allow limited, web-only access

☐ Block Access

Apps that don't use modern authentication

This setting applies to third-party apps and Office 2010 and earlier.

☒ Allow

☐ Block


Control access based on network location





☐ Only allow access from specific IP address locations

Sean Metcalf (@PyroTek3) TrimarcSecurity.com

OKCancel

SharePoint Data Access Controls

 Office 365 Admin

   Sean Metcalf 

SharePoint admin center

site collections

infopath

user profiles

bcs

term store

records management

search

secure store

apps

sharing

settings

configure hybrid

access control

Sharing outside your organization
Control how users share content with people outside your organization.

☒ Don't allow sharing outside your organization
☐ Allow sharing only with the external users that already exist in your organization's directory
☐ Allow users to invite and share with authenticated external users
☐ Allow sharing to authenticated external users and using anonymous access links

Default link type
Choose the type of link that is created by default when users get links. [Learn more.](#)

☐ Direct - only people who have permission
☒ Internal - people in the organization only
☐ Anonymous Access - anyone with the link


Default link permission
Choose the default permission that is selected when users share. This applies to anonymous access, internal and direct links.





☐ View
☒ Edit

OK

Cancel

SharePoint Data Access Controls

 Office 365 Admin

   Sean Metcalf 

SharePoint admin center

site collections

infopath

user profiles

bcs

term store

records management

search

secure store

apps

sharing

settings

configure hybrid

access control

Sharing outside your organization

Control how users share content with people outside your organization.

- ☐ Don't allow sharing outside your organization
- ☒ Allow sharing only with the external users that already exist in your organization's directory
- ☐ Allow users to invite and share with authenticated external users
- ☐ Allow sharing to authenticated external users and using anonymous access links

Who can share outside your organization

- ☐ Let only users in selected security groups share with authenticated external users

Default link type

Choose the type of link that is created by default when users get links. [Learn more.](#)

- ☐ Direct - only people who have permission
- ☒ Internal - people in the organization only
- ☐ Anonymous Access - anyone with the link

Default link permission

Choose the default permission that is selected when users share. This applies to anonymous access, internal and direct links.

- ☐ View
- ☒ Edit

Additional settings

- ☐ Limit external sharing using domains (applies to all future sharing invitations). Separate multiple domains with spaces. [Learn more.](#)
- ☐ Prevent external users from sharing files, folders, and sites that they don't own
- ☐ External users must accept sharing invitations using the same account that the invitations were sent to
- ☐ Require recipients to continually prove account ownership when they access shared items

Notifications

E-mail OneDrive for Business owners when

- ☒ Other users invite additional external users to shared files
- ☒ External users accept invitations to access files
- ☒ An anonymous access link is created or changed

Sean Metcalf (@PyroTek3) TrimarcSecurity.com