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
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

- Server
- Domain
- Domain Admin
- Pass the Hash
- Private IPs
- RDP / SSH

- Services
- Subscription
- Subscription Admin
- Credential Pivot
- Public IPs
- Management APIs

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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Managing VMs is Still Your Responsibility...

Casey Smith @subTee

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

#PrivEsc https://pbs.twimg.com/media/DFH8yMKUIAAO1h.jpg
Microsoft have a website called docs.com where Office 365 customers can share anything in public. It has a search function.
Kevin Beaumont • @GossiTheDog • Mar 26

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

Accounts - Docs.com
https://docs.com › rebecca-lim-1 › account...

Hostname: leadsgoal.ip-zone.com Username: leadsgoal
Password: f21b9315 ... samantha.kreative@gmail.com
bpcs2015 VPN: France Post Code : 75001 LI ...

System Setup Checklist - Docs.com
https://docs.com › dan-van-malsen › syst...

Content published by Dan Van Malsen about System
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

Whoops! Sensitive intelligence data potentially disclosed…
BLAME HUMAN ERROR FOR WWE AND VERIZON'S MASSIVE DATA EXPOSURES

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,
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?

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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)
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
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)
Discover Federation Servers

No standard naming for FS. Some are hosted in the cloud. DNS query for:

- adfs
- auth
- fs
- okta
- ping
- sso
- sts
<table>
<thead>
<tr>
<th>Server</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>Apache-Coyote/1.1</td>
</tr>
<tr>
<td>BigIP</td>
<td></td>
</tr>
<tr>
<td>JPMX</td>
<td></td>
</tr>
<tr>
<td>Kestrel</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/7.5</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/7.5,6.0</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/7.5</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/7.5</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/8.0</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/8.5</td>
<td></td>
</tr>
<tr>
<td>Microsoft-IIS/8.5</td>
<td></td>
</tr>
<tr>
<td>Microsoft-HTTPAPI/2.0</td>
<td></td>
</tr>
<tr>
<td>Microsoft-HTTPAPI/2.0</td>
<td></td>
</tr>
<tr>
<td>nginx</td>
<td></td>
</tr>
<tr>
<td>Oracle-iPlanet-Web-Server/7.0</td>
<td></td>
</tr>
<tr>
<td>WebSEAL/7.0.0.8 (Build 160317)</td>
<td></td>
</tr>
</tbody>
</table>

```
TiPMix=0.505320029568542; path=/; Domain=okta.**********;
En1L; expires=Wed, 11-Oct-2017 17:06:46 GMT; Max-Age=7776000; path=/; domain=
```
## Federation Server Certificate Info

### Server Key and Certificate #1

<table>
<thead>
<tr>
<th>Subject</th>
<th>Fingerprint SHA256: 152151b3874126b64b65f206f2771e927208874932420b578874968671</th>
<th>Fingerprint SHA1: 978576a0697708f281469b207120b2593053c6835f32420b578874968671</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common names</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternative names</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>0c0699b7d788996f206f2771e927208874932420b578874968671</td>
<td>0c0699b7d788996f206f2771e927208874932420b578874968671</td>
</tr>
<tr>
<td>Valid from</td>
<td>Fri, 09 Dec 2016 00:00:00 UTC</td>
<td>Fri, 09 Dec 2016 00:00:00 UTC</td>
</tr>
<tr>
<td>Valid until</td>
<td>Thu, 25 Jan 2018 12:00:00 UTC (expires in 9 years)</td>
<td>Thu, 25 Jan 2018 12:00:00 UTC (expires in 9 years)</td>
</tr>
<tr>
<td>Key</td>
<td>EC 256 bits</td>
<td>EC 256 bits</td>
</tr>
<tr>
<td>Weak key (Debian)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Issuer</td>
<td>DigiCert SHA2 High Assurance Server CA</td>
<td>DigiCert SHA2 High Assurance Server CA</td>
</tr>
<tr>
<td>Signature</td>
<td>SHA256withRSA</td>
<td>SHA256withRSA</td>
</tr>
<tr>
<td>Extended Validation</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Certificate Transparency</td>
<td>Yes (certificate)</td>
<td>Yes (certificate)</td>
</tr>
<tr>
<td>OCSP Must Staple</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Revocation</td>
<td>Good (not revoked!)</td>
<td>Good (not revoked!)</td>
</tr>
<tr>
<td>DNS CAA</td>
<td>No (more info)</td>
<td>Yes (more info)</td>
</tr>
<tr>
<td>Trusted</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Configuration

#### Protocols

- TLS 1.3: Yes
- 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_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (256 bits)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (256 bits)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (256 bits)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (256 bits)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (256 bits)
- TLS_RSA_WITH_AES_256_CBC_SHA (256 bits)
- TLS_ECDH_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (256 bits)
- TLS_ECDH_RSA_WITH_CHACHA20_POLY1305_SHA256 (256 bits)

*Sean Metcalf (@PyroTek3) TrimarcSecurity.com*
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 ≈ KRBTGT (think Golden Tickets)
Similar to a golden ticket attack, if we have the key that signs the object which holds the user’s identity and permissions (\textit{KRB TGT} 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 \textit{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 \textit{private key} is \textit{not renewed} automatically
- Changing a user’s password won’t affect the generated SAML

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  

• Azure Cloud Shell (in browser BASH or PowerShell shell)
Get-MsolCompanyInformation

DisplayName: International Genetic Technologies
PreferredLanguage: en
Street: 100 Farallon Road
City: Palo Alto
State: CA
PostalCode: 94301
Country: US
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:
LastPasswordSynchronizationEnabled: False

Get-MsolGroup

<table>
<thead>
<tr>
<th>ObjectId</th>
<th>DisplayName</th>
<th>GroupType</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>912f339b-a375-4747-8fe6-c5957e9e93a3</td>
<td>InGen Systems Admins</td>
<td>Security</td>
<td>Unix System Admins</td>
</tr>
<tr>
<td>12579f70-0287-4ac6-a0d5-89ce5312a8f4</td>
<td>InGen Security</td>
<td>Security</td>
<td>Security Team</td>
</tr>
<tr>
<td>6a4e110c-5434-4586-876b-34b529432ace</td>
<td>InGen R&amp;D</td>
<td>Security</td>
<td>R&amp;D</td>
</tr>
<tr>
<td>26248498-4769-463f-b164-94255de18e4c</td>
<td>InGen Dino Team</td>
<td>Security</td>
<td>Dino Team</td>
</tr>
<tr>
<td>a3de767a-0f04-4b2a-ac1d-0d0160358dec</td>
<td>AAD DC Administrators</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>868545b6-1579-45e2-8839-ab68e0ab6017</td>
<td>Password Reset Group</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>af72c0d8-f19f-48ba-a6c6-0c6d7d084ef</td>
<td>InGenPasswordResetGroup</td>
<td>Security</td>
<td></td>
</tr>
</tbody>
</table>

Name: starkindustriestech.net
cyberdynesys.net
ingentech.co

AvailabilityStatus: Managed
AuthenticationType: Managed
AAD – Microsoft 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 utalize 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 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:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
<tr>
<td>Read/Write all properties User</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties iNetOrgPerson</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Group</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Read/Write all properties Contact</td>
<td>Import and Exchange hybrid</td>
</tr>
<tr>
<td>Reset password</td>
<td>Preparation for enabling password writeback</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replicate Directory Changes</td>
<td>Password sync</td>
</tr>
<tr>
<td>Replicate Directory Changes All</td>
<td></td>
</tr>
</tbody>
</table>

| 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  |

DEF CON 25 (July 2017)
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-1-5-21-2578996962-4185879466-369690401-500
Object Relative ID : 500

Credentials:
  Hash NTLM: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 0: 96ae239ae1f8f186a205b6863a3c955f
    ntlm- 1: 5164b7a0fdaf36d56739954bbbc23835
    ntlm- 2: 7c08d63a2f48f045971bc2236edf3f3ac
    lm - 0: 6cf3d3clc30b3fe5d716efef10f46e49
    lm - 1: d1726cc03fbb143869304c6d3f30f2db8d

Supplemental Credentials:
  * Primary:Kerberos-Newer-Keys *
    Default Salt : RD.ADSECURITY.ORGAdmin
    Default Iterations : 4096
    Credentials
      aes256_hmac (4096) : 2394f3a0f5bc0b5779bfc610e5d845e78638deac142e3674af58a674b67e102b
      aes128_hmac (4096) : f4d4a882350f5b5c4f176d418af2b2a
      des_cbc_md5 (4096) : 5d8c9e464a4dad4ac
      rc4_plain (4096) : 96ae239ae1f8f186a205b6863a3c955f
    OldCredentials
      aes256_hmac (4096) : 0526e75306d2090d03f0ea0e0f681aae5ae591e29d27ea493c3322525382dd3f
      aes128_hmac (4096) : 4c41e4d7a3e932d64feeed264d48a19e
      des_cbc_md5 (4096) : 5bf0d0e1e3e2334
      rc4_plain (4096) : 5164b7a0fdaf36d56739954bbbc23835
```
# Custom Permissions for Azure AD Connect

<table>
<thead>
<tr>
<th>Feature</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>msDS-ConsistencyGuid feature</td>
<td>Write permissions to the msDS-ConsistencyGuid attribute documented in <a href="https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions">Design Concepts - Using msDS-ConsistencyGuid as sourceAnchor</a>.</td>
</tr>
</tbody>
</table>
| Password sync                                | • Replicate Directory Changes  
• Replicate Directory Changes All                                      |
| Exchange hybrid deployment                   | Write permissions to the attributes documented in [Exchange hybrid writeback](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions) for users, groups, and contacts. |
| Exchange Mail Public Folder                  | Read permissions to the attributes documented in [Exchange Mail Public Folder](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions) for public folders. |
| Password writeback                           | Write permissions to the attributes documented in [Getting started with password management](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions) for users. |
| Device writeback                             | Permissions granted with a PowerShell script as described in [device writeback](https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions). |
| 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.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admins</td>
<td>Security Group</td>
<td>Legacy Administrators Group</td>
</tr>
<tr>
<td>AWS Delegated Account Operators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Add Workstations To Domain Users</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Domain Name System Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Dynamic Host Configuration Protocol Admin</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Enterprise Certificate Authority Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Group Policy Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Kerberos Delegation Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Managed Service Account Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Remote Access Service Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Replicate Directory Changes Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Server Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Sites and Services Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated Terminal Server Licensing Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>AWS Delegated User Principal Name Sufffix Administrators</td>
<td>Security Group</td>
<td>AWS Provided Group: M...</td>
</tr>
<tr>
<td>Amazon AWS Directory (Active Directory)</td>
<td>Microsoft Azure AD Domain Services</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2 DFL/FFL</td>
<td>Windows Server 2012 R2 DFL/FFL</td>
<td></td>
</tr>
<tr>
<td>Designed for Cloud and Corporate workloads.</td>
<td>Designed for Azure VM joins (primarily).</td>
<td></td>
</tr>
<tr>
<td>Support for trusts including resource forest. Schema updates supported (LDIF import).</td>
<td>Trusts are not supported. No schema updates.</td>
<td></td>
</tr>
<tr>
<td>Ability to spin up additional DCs in different geographic locations.</td>
<td>Standard 2 DCs in a single virtual network in Azure</td>
<td></td>
</tr>
<tr>
<td>Password sync not supported.</td>
<td>Supports password sync from production AD.</td>
<td></td>
</tr>
<tr>
<td>5 Fine-grained Password Policies available for modification to manage password policies.</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>O365 integration support: install Azure AD Connect, ADFS, etc.</td>
<td>Integration with Azure AD.</td>
<td></td>
</tr>
<tr>
<td>Domain join at VM instance creation.*</td>
<td>Pricing: ~$80 - $100/month</td>
<td></td>
</tr>
<tr>
<td>Pricing: ~$80 - $280/month</td>
<td>As of 10/31/2017</td>
<td></td>
</tr>
</tbody>
</table>

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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:
[***] 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.

Microsoft’s official response is to use Microsoft provided MFA, which produce an enormous amount of O365 customers in a difficult state. Most customers see...

Other fun facts about EWS:

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

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_T3LLlUIU
Access Defaults

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

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)

1. Request unicodePWD via MC-DBSR
2. MD5 (unicodePWD)
3. Password sync agent decrypts MD5 envelope to retrieve MD4 hash
4. 8-byte binary hash is converted to 64-byte binary.
5. 10-byte salt added.
6. 64-bit hash is input into SHA256.
7. SHA256 hash sent to Azure AD
8. User signs into Azure AD. If their hashed password matches the stored password then the user is authenticated.


Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Others?

Still researching...
Office 365 Auditing & Logging
Search the audit log in the Office 365 Security & Compliance Center

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:

<table>
<thead>
<tr>
<th>File and page activities</th>
<th>Folder activities</th>
<th>Sharing and access request activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization activities</td>
<td>Site administration activities</td>
<td>Exchange mailbox activities</td>
</tr>
<tr>
<td>Sway activities</td>
<td>User administration activities</td>
<td>Azure AD group administration activities</td>
</tr>
<tr>
<td>Application administration activities</td>
<td>Role administration activities</td>
<td>Directory administration activities</td>
</tr>
<tr>
<td>eDiscovery activities</td>
<td>Power BI activities</td>
<td>Microsoft Teams activities</td>
</tr>
<tr>
<td>Yammer activities</td>
<td>Exchange admin activities</td>
<td></td>
</tr>
</tbody>
</table>

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Search the audit log in the Office 365 Security & Compliance Center

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.
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

```powershell
Import-PSSession $Session
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

```powershell
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
```

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Search the audit log in the Office 365 Security & Compliance Center

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.

<table>
<thead>
<tr>
<th>Friendly name</th>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added delegate mailbox permissions</td>
<td>AddMailboxPermission</td>
<td>An administrator assigned the FullAccess mailbox permission to a user (known as a delegate) 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.</td>
</tr>
<tr>
<td>Copied messages to another folder</td>
<td>Copy</td>
<td>A message was copied to another folder.</td>
</tr>
<tr>
<td>Created or received messages</td>
<td>Create</td>
<td>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.</td>
</tr>
<tr>
<td>Deleted messages from Deleted items folder</td>
<td>SoftDelete</td>
<td>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.</td>
</tr>
<tr>
<td>Moved messages to another folder</td>
<td>Move</td>
<td>A message was moved to another folder.</td>
</tr>
<tr>
<td>Moved messages to Deleted items folder</td>
<td>MoveToDeletedItems</td>
<td>A message was deleted and moved to the Deleted Items folder.</td>
</tr>
<tr>
<td>Purged messages from the mailbox</td>
<td>HardDelete</td>
<td>A message was purged from the Recoverable Items folder (permanently deleted from the mailbox).</td>
</tr>
<tr>
<td>Removed delegate mailbox permissions</td>
<td>RemoveMailboxPermission</td>
<td>An administrator removed the FullAccess permission (that was assigned to a delegate) from a person’s mailbox. After</td>
</tr>
</tbody>
</table>
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.
<table>
<thead>
<tr>
<th>Admin</th>
<th>Delegate</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create (Calendar, Contacts, Notes, or Tasks)</td>
<td>Create (Calendar, Contacts, Notes, or Tasks)</td>
<td>Create (Calendar, Contacts, Notes, or Tasks)</td>
</tr>
<tr>
<td>FolderBind (mailbox open)</td>
<td>FolderBind (mailbox open)</td>
<td></td>
</tr>
<tr>
<td>HardDelete (purged from the Recoverable Items)</td>
<td>HardDelete (purged from the Recoverable Items)</td>
<td>HardDelete (purged from the Recoverable Items)</td>
</tr>
<tr>
<td>MessageBind (message viewed in preview pane or opened)</td>
<td></td>
<td>MailboxLogin</td>
</tr>
<tr>
<td>Move</td>
<td>Move</td>
<td>Move</td>
</tr>
<tr>
<td>MoveToDeletedItems</td>
<td>MoveToDeletedItems</td>
<td>MoveToDeletedItems</td>
</tr>
<tr>
<td>SendAs</td>
<td>SendAs</td>
<td></td>
</tr>
<tr>
<td>SendOnBehalf</td>
<td>SendOnBehalf</td>
<td></td>
</tr>
<tr>
<td>SoftDelete</td>
<td>SoftDelete</td>
<td>SoftDelete</td>
</tr>
<tr>
<td>Update</td>
<td>Update</td>
<td>Update</td>
</tr>
</tbody>
</table>

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Enable Office 365 Mailbox Auditing


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*

<table>
<thead>
<tr>
<th>Name</th>
<th>JArnold</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuditEnabled</td>
<td>True</td>
</tr>
<tr>
<td>AuditLogAgeLimit</td>
<td>90.00:00:00</td>
</tr>
<tr>
<td>AuditAdmin</td>
<td>{Update, Move, MoveToDeletedItems, SoftDelete...}</td>
</tr>
<tr>
<td>AuditDelegate</td>
<td>{Update, SoftDelete, HardDelete, SendAs...}</td>
</tr>
<tr>
<td>AuditOwner</td>
<td>{SoftDelete, HardDelete, MailboxLogin}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>jhammond</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuditEnabled</td>
<td>True</td>
</tr>
<tr>
<td>AuditLogAgeLimit</td>
<td>90.00:00:00</td>
</tr>
<tr>
<td>AuditAdmin</td>
<td>{Update, Move, MoveToDeletedItems, SoftDelete...}</td>
</tr>
<tr>
<td>AuditDelegate</td>
<td>{Update, SoftDelete, HardDelete, SendAs...}</td>
</tr>
<tr>
<td>AuditOwner</td>
<td>{SoftDelete, HardDelete, MailboxLogin}</td>
</tr>
</tbody>
</table>
Monitor App Registrations

To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

<table>
<thead>
<tr>
<th>DISPLAY NAME</th>
<th>APPLICATION TYPE</th>
<th>APPLICATION ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD Domain Services Sync</td>
<td>Web app / API</td>
<td>c9816c72-abe6-4313-b495-ff76...</td>
</tr>
</tbody>
</table>
Microsoft Cloud Logging

- **Azure AD Logging** – Azure AD events – logons, user modification, password changes, administrator activity, etc.
- **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.

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

#### Enterprise applications
- Users can consent to apps accessing company data on their behalf: **Yes**
- Users can add gallery apps to their Access Panel: **Yes**

#### App registrations
- Users can register applications: **Yes**

#### External users
- Guest users permissions are limited: **Yes**
- Admins and users in the guest inviter role can invite: **Yes**
- Members can invite: **Yes**
- Guests can invite: **Yes**

#### Administration portal
- Restrict access to Azure AD administration portal: **Yes**
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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.

View: Sign-in allowed users  Multi-Factor Auth status

<table>
<thead>
<tr>
<th>DISPLAY NAME</th>
<th>USER NAME</th>
<th>MULTI-FACtor AUTH STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Arnold</td>
<td><a href="mailto:JArnold@ingentech.co">JArnold@ingentech.co</a></td>
<td>Disabled</td>
</tr>
<tr>
<td>John Hammond</td>
<td><a href="mailto:jhammond@ingentech.co">jhammond@ingentech.co</a></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Enable MFA for all admins

```powershell
$UserCredential = Get-Credential
Import-Module MSOnline
Connect-MsolService -Credential $UserCredential

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

$sauth.State = "Enabled"

$sauth.RememberDevicesNotIssuedBefore = (Get-Date)

# Enable MFA on all users
Get-MsolUser -All | where {($_.userprincipalname -like "*admin*"}) |        
Foreach {Set-MsolUser -UserPrincipalName $_.UserPrincipalName -StrongAuthenticationRequirements $sauth }
```
Recommended for you

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

View recommendation
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.
Administration:
Who has admin rights?

<table>
<thead>
<tr>
<th>ObjectId</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>729827e3-9c14-49f7-bb1b-9608f156bb8</td>
<td>Helpdesk Administrator</td>
</tr>
<tr>
<td>f023fd81-a637-4b56-95fd-791ac0226033</td>
<td>Service Support Administrator</td>
</tr>
<tr>
<td>b0f54661-2d74-4c50-a0a3-1ec803f12efe</td>
<td>Billing Administrator</td>
</tr>
<tr>
<td>b5468a13-3945-4a40-b0b1-5d78c2676bbf</td>
<td>Mailbox Administrator</td>
</tr>
<tr>
<td>4ba39ca4-527c-499a-b93d-d9b492c50246</td>
<td>Partner Tier1 Support</td>
</tr>
<tr>
<td>e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8</td>
<td>Partner Tier2 Support</td>
</tr>
<tr>
<td>88d8e3e3-8f55-4a1e-953a-9b9898b876b</td>
<td>Directory Readers</td>
</tr>
<tr>
<td>29232dfc-9323-42fd-ade2-1d097af3e4de</td>
<td>Exchange Service Administrator</td>
</tr>
<tr>
<td>75941009-915a-4869-ab7e-691bff18279e</td>
<td>Lync Service Administrator</td>
</tr>
<tr>
<td>fe9300e7-5e62-47db-91af-98c3a49a3b1</td>
<td>User Account Administrator</td>
</tr>
<tr>
<td>9360fceb-5f1b-4baa-8175-e2a00bac4301</td>
<td>Directory Writers</td>
</tr>
<tr>
<td>6e90394-6f95-4237-9190-01217145e10</td>
<td>Company Administrator</td>
</tr>
<tr>
<td>d65e002d-0214-4654-8e5d-766fb330e2c0</td>
<td>Email Verified User Creator</td>
</tr>
<tr>
<td>eb1d8c34-acf5-456d-8424-c1f1a6f6db85</td>
<td>ADHoc License Administrator</td>
</tr>
<tr>
<td>f28a1f50-6f67-4571-818b-6a12f2a6fb6c</td>
<td>SharePoint Service Administrator</td>
</tr>
<tr>
<td>d405c6df-0af8-4e3b-95e4-4d06e542189e</td>
<td>Device Users</td>
</tr>
<tr>
<td>9f0620ad-73c1-4d4c-880a-6ed90606fd8</td>
<td>Device Administrators</td>
</tr>
<tr>
<td>9c09495-4995-41c8-84c8-3eb9b32c9f3</td>
<td>Device Join</td>
</tr>
<tr>
<td>c34f683f-4d5a-4403-affd-6615e00e3a7f</td>
<td>Workplace Device Join</td>
</tr>
<tr>
<td>17315797-102d-40b4-93e0-432062caca18</td>
<td>Compliance Administrator</td>
</tr>
<tr>
<td>d29b2b05-8046-44ba-8758-1e26182f5f32</td>
<td>Directory Synchronization Accounts</td>
</tr>
<tr>
<td>2b4f9bcd-da44-4968-8aec-78e1674fa64d</td>
<td>Device Managers</td>
</tr>
<tr>
<td>9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c5</td>
<td>Application Administrator</td>
</tr>
<tr>
<td>cfc138e5-3621-4004-a7cb-879624cedc7c</td>
<td>Application Developer</td>
</tr>
<tr>
<td>5d6b6b7-7de1-4623-b4af-96380a352509</td>
<td>Security Reader</td>
</tr>
<tr>
<td>194ae4cb-b12b-40b2-bd5b-6091b380977d</td>
<td>Security Administrator</td>
</tr>
<tr>
<td>e8611a8-b189-4e68-94e1-60213a1b8f14</td>
<td>Privileged Role Administrator</td>
</tr>
<tr>
<td>3a2c62db-5318-420d-8d74-23affee5d9d5</td>
<td>Intune Service Administrator</td>
</tr>
<tr>
<td>158c047a-c907-4556-b7ef-446551a6b5f7</td>
<td>Cloud Application Administrator</td>
</tr>
<tr>
<td>5cf4f9dc-47dc-4cf7-8c9a-9e4207cfbc91</td>
<td>Customer LockBox Access Approver</td>
</tr>
<tr>
<td>44367163-eba1-44c3-98af-f5787879f96a</td>
<td>CRM Service Administrator</td>
</tr>
<tr>
<td>a9ea8996-122f-4c74-9520-8edc192826c</td>
<td>Power BI Service Administrator</td>
</tr>
<tr>
<td>95e79109-95c0-4d8e-aee3-d01accf2d47b</td>
<td>Guest Inviter</td>
</tr>
<tr>
<td>b1be1c3e-b68b-4f19-8427-6fa0d97fe9b</td>
<td>Conditional Access Administrator</td>
</tr>
<tr>
<td>4a5d8f65-41da-4d4e-8968-e035b65339cf</td>
<td>Reports Reader</td>
</tr>
<tr>
<td>Office 365 admin role</td>
<td>Translates to this in Exchange Online ...</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Global Admin</td>
<td>Exchange Online admin</td>
</tr>
<tr>
<td>Billing admin</td>
<td>N/A</td>
</tr>
<tr>
<td>Password admin</td>
<td>Help Desk admin*</td>
</tr>
<tr>
<td>Service admin</td>
<td>N/A</td>
</tr>
<tr>
<td>User management admin</td>
<td>N/A</td>
</tr>
<tr>
<td>Exchange administrator</td>
<td>Exchange Online admin</td>
</tr>
<tr>
<td>SharePoint administrator</td>
<td>N/A</td>
</tr>
<tr>
<td>Skype for Business administrator</td>
<td>N/A</td>
</tr>
<tr>
<td>Compliance administrator</td>
<td>Organization Management</td>
</tr>
</tbody>
</table>

*Help Desk admin is synonymous with the Password admin role.
import-module Msonline
$O365Roles = Get-MsoRole
ForEach ($O365RoleItem in $O365Roles)
{
    $RoleMembers = Get-MsoRoleMember -RoleObjectId $O365RoleItem.ObjectId
    IF ($RoleMembers)
    {
        Write-output " $(O365RoleItem.Name): "
        $RoleMembers | Format-Table RoleMemberType,EmailAddress,DisplayName -AutoSize
    }
}
Improving Office 365 Security: Secure Score

Your Secure Score

Secure Score figures out what Office 365 services you are using, then looks at your configuration and behaviors and compares it to a baseline asserted by Microsoft. If your configuration and behaviors are in line with best practices, you will get points, which you can track over time. More importantly, you will be able to quickly determine what things you can do to reduce their risk.

Your Secure Score Summary

Your Secure Score is:

25

Of 364

Take action to see how you can improve your score today.

Your Secure Score is:

248

Of 483

Your Secure Score is:

25

Of 364

Take Action. Improve Your Score
Improving Office 365 Security: Secure Score

Your Secure Score

Secure Score figures out what Office 365 services you are using, then looks at your configuration and behaviors and compares it to a baseline asserted by Microsoft. If your configuration and behaviors are in line with best practices, you will get points, which you can track over time. More importantly, you will be able to quickly determine what things you can do to reduce their risk.

Your Secure Score Summary

Your Secure Score is:

25

Of 364

Take action to see how you can improve your score today.

For more information about your Secure Score go to: Score Analyzer.

What’s new

We have introduced the fully remediated workflows for the following controls. Check it out!

- Check out the new ignore action and third-party antivirus feature!
- Enable Client Rules Forwarding
- Set outbound email notifications
- Enable customer access feature
- Designate more than one tenant admin
- Designate less than 5 tenant admins
- Use non-global administrative role

Risk assessment

The following threats could be mitigated by taking the recommended Secure Score actions:

- Account Brute
<table>
<thead>
<tr>
<th>Action Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MFA for all global admins</td>
<td></td>
</tr>
<tr>
<td>Enable MFA for all users</td>
<td></td>
</tr>
<tr>
<td>[Not Scored] Enable audit data recording</td>
<td></td>
</tr>
<tr>
<td>Enable Client Rules Forwarding Block</td>
<td></td>
</tr>
<tr>
<td>Advanced Action</td>
<td></td>
</tr>
<tr>
<td>Review signs-ins after multiple failures report weekly</td>
<td></td>
</tr>
<tr>
<td>[Not Scored] Set outbound spam notifications</td>
<td></td>
</tr>
<tr>
<td>Enable mailbox auditing for all users</td>
<td></td>
</tr>
<tr>
<td>Review sign-ins from unknown sources report weekly</td>
<td></td>
</tr>
<tr>
<td>Review signs-ins from multiple geographies report weekly</td>
<td></td>
</tr>
<tr>
<td>Review role changes weekly</td>
<td></td>
</tr>
<tr>
<td>Store user documents in OneDrive for Business</td>
<td></td>
</tr>
<tr>
<td>[Not Scored] Enable Information Rights Management (IRM) services</td>
<td></td>
</tr>
<tr>
<td>Use audit data</td>
<td></td>
</tr>
</tbody>
</table>

*Your pending Secure Score is: 316*
# 27 Actions in the queue

<table>
<thead>
<tr>
<th>Category</th>
<th>Action Type</th>
<th>User Impact</th>
<th>Implementation Cost</th>
<th>Control Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>Behavior</td>
<td>Low</td>
<td>Low</td>
<td>Advanced</td>
<td>[Not Scored] Set outbound spam notifications</td>
</tr>
<tr>
<td>Data</td>
<td>Configuration</td>
<td>High</td>
<td>High</td>
<td>Standard</td>
<td>Enable mailbox auditing for all users</td>
</tr>
<tr>
<td>Device</td>
<td>Review</td>
<td>Moderate</td>
<td>Moderate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Your pending Secure Score is: 316
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

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

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’

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.
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.

### Threats
- Account Breach

<table>
<thead>
<tr>
<th>Action Category</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Impact</td>
<td>Low</td>
</tr>
<tr>
<td>Implementation Cost</td>
<td>Low</td>
</tr>
<tr>
<td>Action Score</td>
<td>0/10</td>
</tr>
</tbody>
</table>
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."

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
## Security Center - Overview

### Overview
- **Recommendations**: 4 Total
- **Security solutions**: 1 Total
- **New alerts & incidents**: 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)**
  - 31 Dec

### Adaptive application controls (Preview)
- **Protected VMs**: 0
- **Approved resources**: 0
- **Enable Application Whitelisting**: [Link]
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Resources</th>
<th>Current Pricing Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay-As-You-Go</td>
<td>0 applicable resources</td>
<td>Free</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>0 applicable resources</td>
<td>Free</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>0 applicable resources</td>
<td>Free</td>
</tr>
<tr>
<td>Pay-As-You-Go</td>
<td>0 applicable resources</td>
<td>Free</td>
</tr>
</tbody>
</table>

Apply Standard plan
First 60 days are free!
## Security Center - Recommendations

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>RESOURCE</th>
<th>STATE</th>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Protection not installed on Azure VMs</td>
<td>InGenAdmin1</td>
<td>Open</td>
<td>High</td>
</tr>
<tr>
<td>Apply a Just-In-Time network access control (preview)</td>
<td>InGenAdmin1</td>
<td>Open</td>
<td>High</td>
</tr>
<tr>
<td>Apply disk encryption</td>
<td>InGenAdmin1</td>
<td>Open</td>
<td>High</td>
</tr>
<tr>
<td>Provide security contact details</td>
<td>1 subscriptions</td>
<td>Open</td>
<td>Medium</td>
</tr>
</tbody>
</table>

---

Security Center Highlights Potential Issues
Connect Additional Data Sources for Better Insight

Security Center - Security solutions

Connected solutions (1)

- Identity protection
  - MICROSOFT
  - Azure AD Identity Protections
  - Connected

Add data sources (3)

- Non-Azure computers
  - MICROSOFT
  - Onboard your non-Azure computers to Azure Security Center and gain security assessment, recommendations and more powerful features

- CEF 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

- Advanced Threat Analytics
  - MICROSOFT
  - Integrate Microsoft Advanced Threat Analytics suspicious activities along with other detections in your environment, and gain correlations and otherwise undetectable

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Adaptive Application Controls

**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:

<table>
<thead>
<tr>
<th>NAME</th>
<th>VM</th>
<th>PROCESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription 1</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>C:\ProgramFiles\Octopus Deploy\Tentacle\Te...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Octopus\Calamar\3.3.13\Octodiff.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\ProgramFiles\Octopus Deploy\Tentacle\Te...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Octopus\Calamar\3.3.13\Octodiff.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\ProgramFiles\Octopus Deploy\Tentacle\Te...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\Octopus\Calamar\3.3.13\Octodiff.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PORT</td>
<td>PROT...</td>
<td>ALLOWED SOUR...</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>-----------------</td>
</tr>
<tr>
<td>22</td>
<td>Any</td>
<td>Per request</td>
</tr>
<tr>
<td>3389</td>
<td>Any</td>
<td>Per request</td>
</tr>
<tr>
<td>5985</td>
<td>Any</td>
<td>Per request</td>
</tr>
<tr>
<td>5986</td>
<td>Any</td>
<td>Per request</td>
</tr>
</tbody>
</table>

Just In Time (JIT) VM Access Configuration

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.
### My Azure AD directory roles

#### Eligible role assignments

<table>
<thead>
<tr>
<th>ROLE NAME</th>
<th>STATUS</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Administrator</td>
<td>Request activation</td>
<td></td>
</tr>
</tbody>
</table>

#### Active role assignments

No roles found

---

**Global Administrator**

**Role activation details**

- **Activate**
- **Deactivate**

**Request role activation**

- **Global Administrator**

- **Reason for role activation**

Need to update global settings as per Hammond.
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)

REQUESTOR: John Arnold
ROLE: Global Administrator
REASON: Company info update.
REQUEST RECEIVED: 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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
Azure AD Identity Protection provides a consolidated view of at-risk accounts and vulnerabilities, allowing for immediate risk remediation and setting policies for future events. It is built on Microsoft's experience protecting consumer identities, providing 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 related information so you can easily understand how risky each user is.

When using the Azure AD Identity Protection, you can get alerts for:

- 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
Enter name

Description
Enter description (optional)

Data source
Choose appliance...

☐ Anonymize private information
Store and display only encrypted usernames.

Choose traffic logs
Choose up to 20 files
1 GB maximum size per log, from the last 90 days

Report creation process
1. Analysis takes up to 24 hours | Track status

- Upload
- Parse
- Data analysis
- Generate report

View sample report
<table>
<thead>
<tr>
<th>Activity</th>
<th>User</th>
<th>App</th>
<th>IP address</th>
<th>Location</th>
<th>Device</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log on</td>
<td>sean</td>
<td>Microsoft...</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Set company information: proper</td>
<td>sean</td>
<td>Office 365</td>
<td>70.21</td>
<td>Other</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.21</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Microsoft...</td>
<td>70.2</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.2</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
<tr>
<td>Log on</td>
<td>Sean Metcalf</td>
<td>Office 365</td>
<td>70.2</td>
<td>United St</td>
<td></td>
<td>Nov 6, 2017</td>
</tr>
</tbody>
</table>
Create activity policy

Policy template
No template*

Policy name
All Admin Activity

Description

Policy severity
Low* 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

Alerts

- Create alert: Use your organization's default settings
  - Daily alert limit: 5
  - Send alert by email
  - Send alert as text message

Governance

- All apps
- Office 365

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

As of 10/2017
Cloud Security Best Practices

You keep using that term, I do not think it means what you think it means.
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.

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
VM Recommendations

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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.
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

Amazon AWS Directory FAQ
https://aws.amazon.com/directoryservice/faqs/

Azure Security Center

Cloud App Security
https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
References

Azure Network Security Best Practices

Azure security best practices and patterns

Azure virtual machine security best practices

Azure identity & access security best practices

Security Best Practices for Windows Azure Solutions - Download Center
http://download.microsoft.com/download/7/8/a/78ab795a-8a5b-48b0-9422-fddeee8f70c1/securitybestpracticesforwindowsazuresolutinsfeb2014.docx

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
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

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

Sean Metcalf (@PyroTek3) TrimarcSecurity.com
O365 SharePoint Controls
SharePoint Data Access Controls

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
SharePoint Data Access Controls

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
SharePoint Data Access Controls

- **Sharing outside your organization**
  - Control how users share content with people outside your organization.
  - Options: Don't allow sharing outside your organization, Allow sharing only with the external users that already exist in your organization's directory.
- **Who can share outside your organization**
  - Option: 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.
  - Options: 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.
  - Options: View, Edit.
- **Additional settings**
  - Limit external sharing using domains (applies to all future sharing invitations).
  - 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.
    - Options: Other users invite additional external users to shared files, External users accept invitations to access files, An anonymous access link is created or changed.