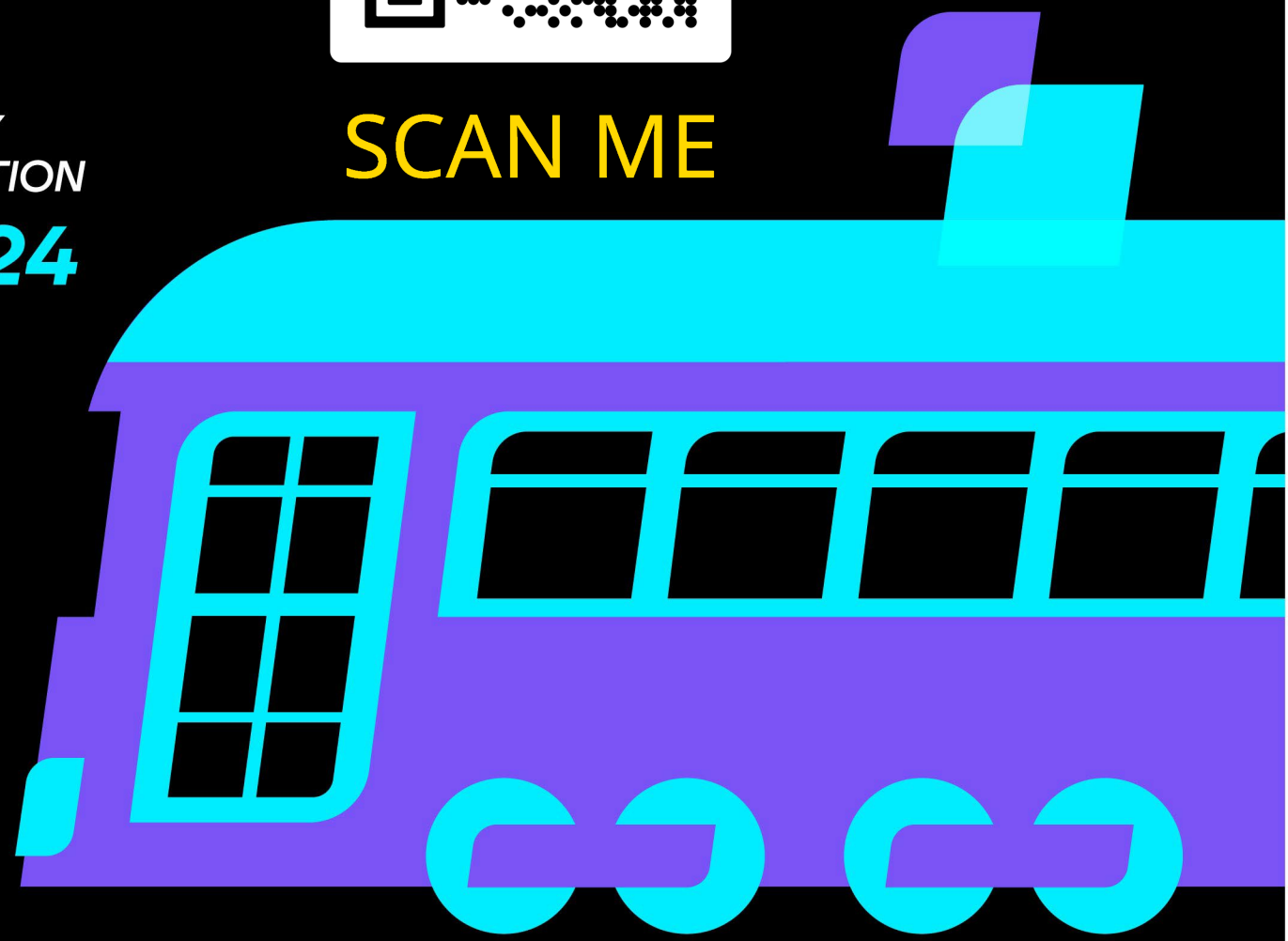




HYBRID  
IDENTITY  
PROTECTION  
**conf24**



**SCAN ME**





# After The Cyberattack - Best Practices for Resynchronizing AD And Entra ID

Jorge de Almeida Pinto  
Senior Incident Response Lead  
SEMPERIS  
[jorged@semperis.com](mailto:jorged@semperis.com)



SCAN ME

# Introducing Me, Myself & I!



**Jorge de Almeida Pinto**  
Senior Incident Response Lead

<b>LinkedIn</b>	<a href="http://tiny.cc/JorgeLinkedIn">http://tiny.cc/JorgeLinkedIn</a>
<b>Blog</b>	<a href="http://tiny.cc/JQFKblog">http://tiny.cc/JQFKblog</a>
<b>Twitter</b>	<a href="http://tiny.cc/JQFKtwitter">http://tiny.cc/JQFKtwitter</a>
<b>Website</b>	<a href="https://www.semperis.com/">https://www.semperis.com/</a>
<b>Blog</b>	<a href="https://www.semperis.com/blog/">https://www.semperis.com/blog/</a>
<b>Podcast</b>	<a href="https://hipconf.libsyn.com/">https://hipconf.libsyn.com/</a>
<b>Contact</b>	<a href="mailto:jorged@semperis.com">jorged@semperis.com</a>



- Technology Focus: Identity, Security And Recovery
- Product Focus: AD, ADFS, Entra Connect/Cloud Sync, FIM/MIM, Entra (ID) Technologies.
- Architecting, designing, implementing and maintaining secure identity solutions
- Writer Of: “KRBTGT Pwd Reset”, “AD Convergence”, “SYSVOL Coverage” Scripts (Feedback WELCOME!)

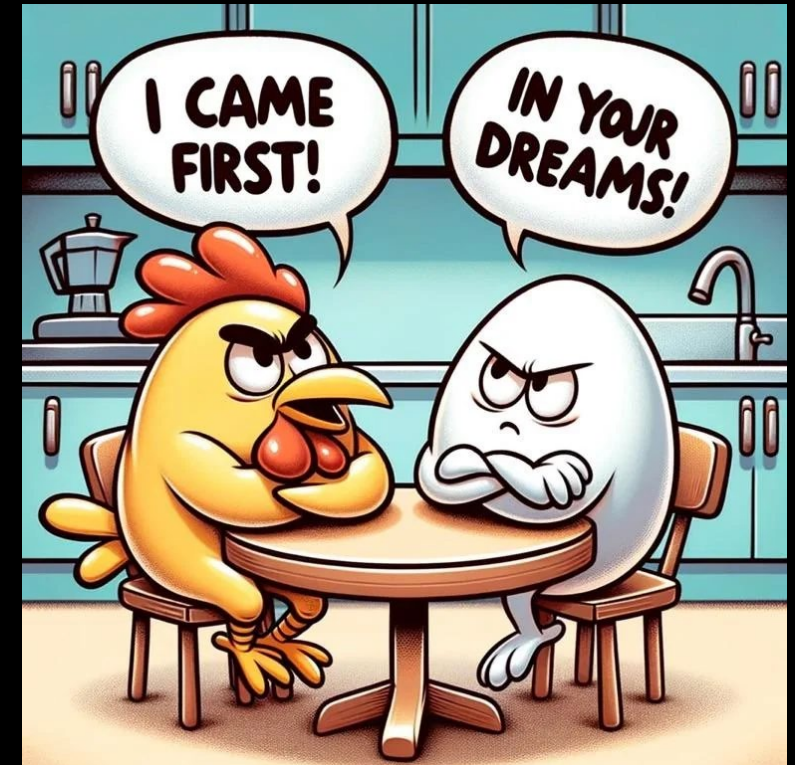
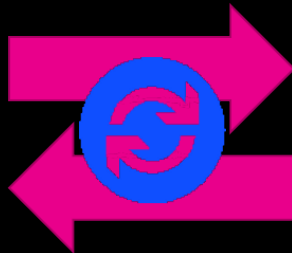


SCAN ME

# Scenario – AD And EID Trashed

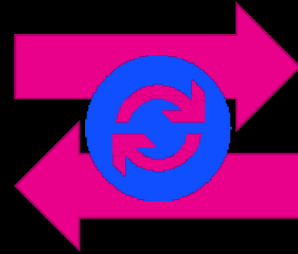
THE WORST THAT CAN HAPPEN

- WHAT GOES FIRST – AND WHY?
  - Recover AD, Sync To EID, Recover Objects In Entra ID? OR
  - Recover Objects In Entra ID, Recover AD, Sync & Match Objects In EID?



# Scenario – Only AD Trashed

LESS WORSE, STILL BAD



# Forest Recovery

## > Backup To Choose/Use

- Any Chosen Backup – Post Attack
    - AD Security MUST BE Assessed
- Going To Production = Recovery + \$

Keep GAP of differences  
as small as possible.  
**!!! SMALLEST IMPACT !!!**  
(Fixing AD Security is easier, than closing GAPS)



Entra ID

- Fix Changes/Mismatches  
In Restored AD Between  
"Today" And...

- Most Recent AD Backup
- Or
- 10 days Old AD Backup



T-10  
(Example)



T-1  
(Example)



T = 0  
(Now)

Time



DELTA

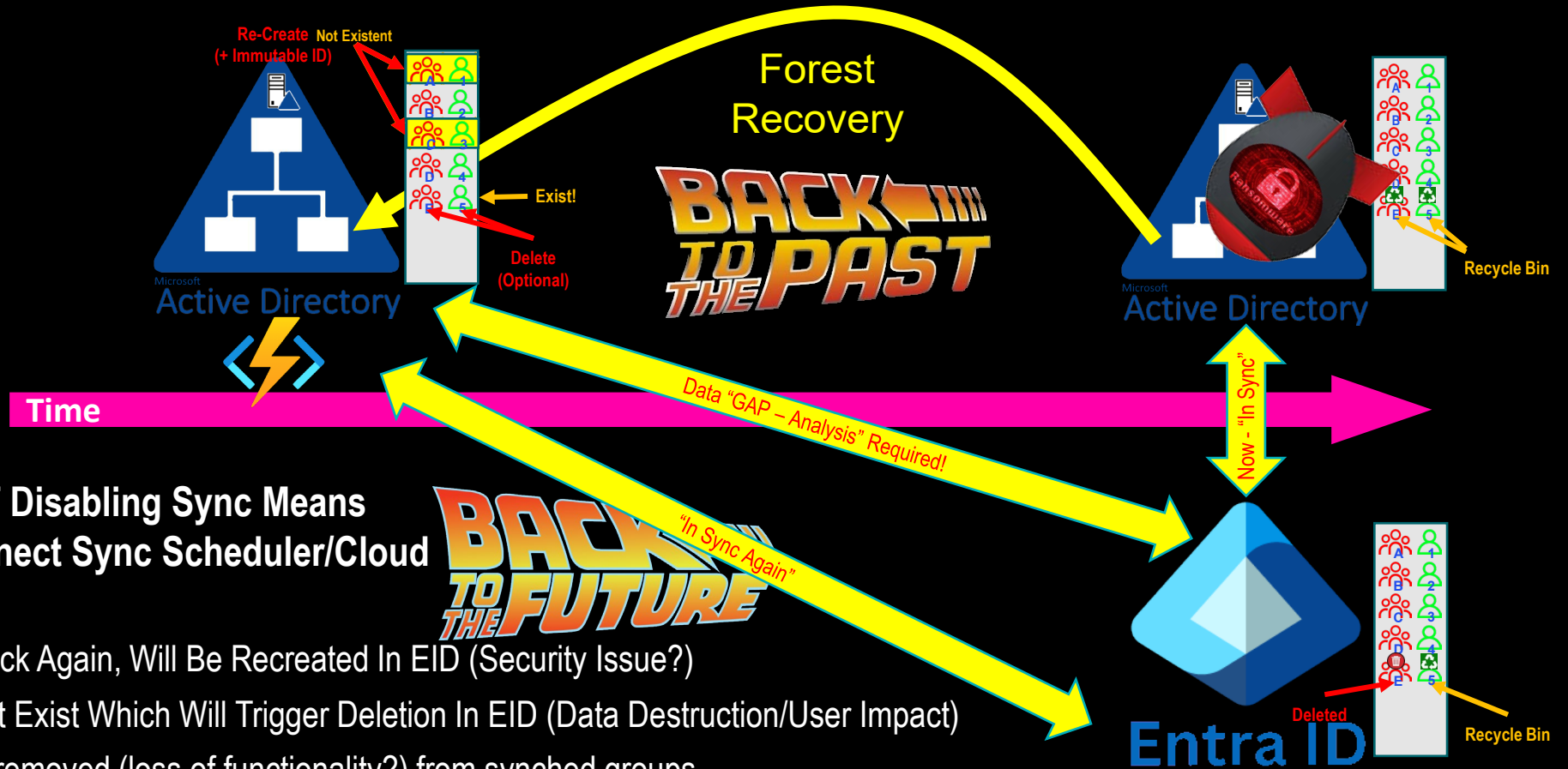
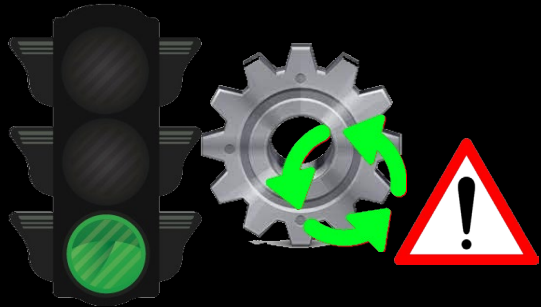


DELTA



# Forest Recovery

## > Impact On Entra ID



- **JUST** Reenabling Sync OR NOT Disabling Sync Means (REMARK: Assumed Entra Connect Sync Scheduler/Cloud Sync Config Is Still Enabled!):

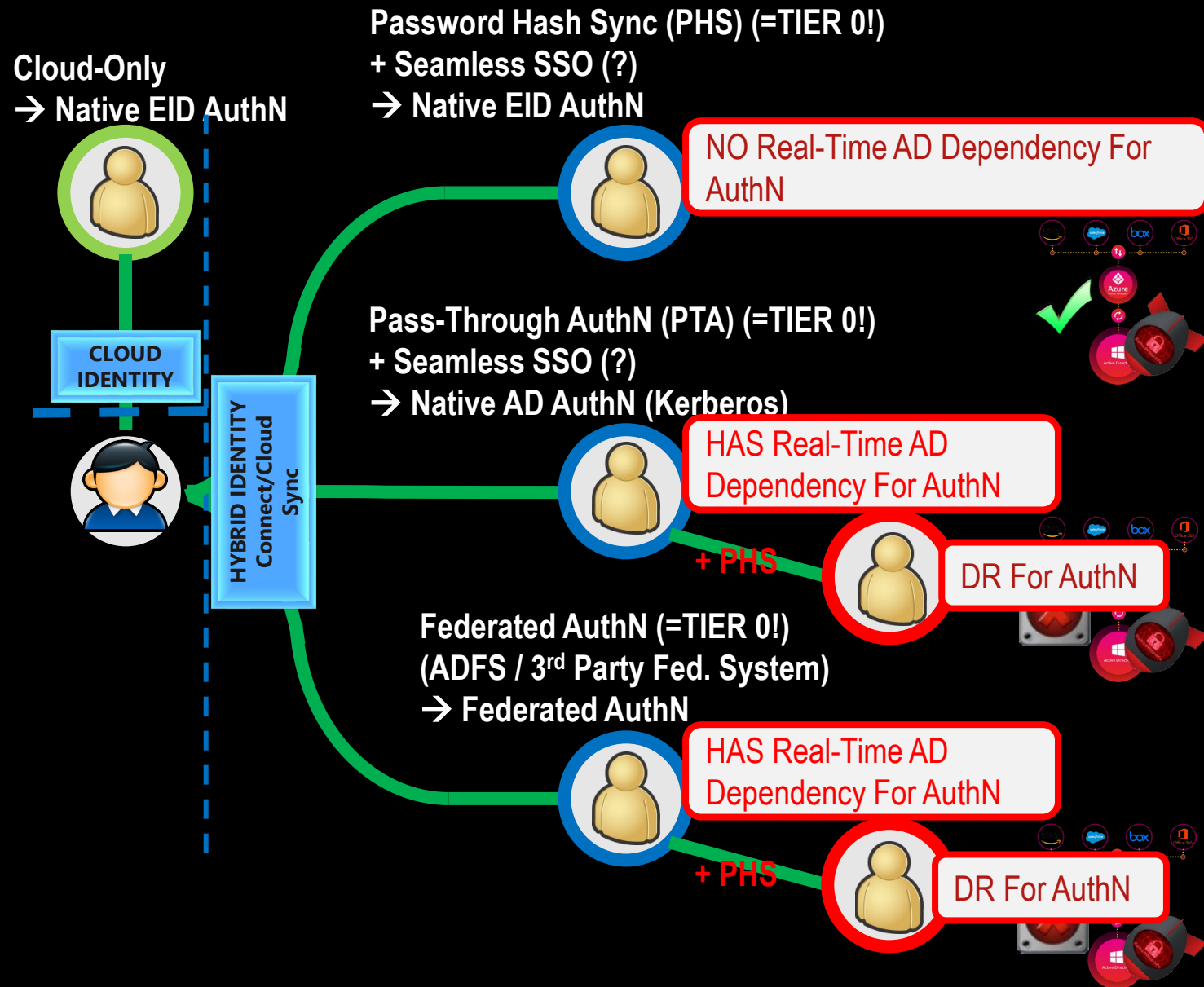
- Previously DELETED Objects Are Back Again, Will Be Recreated In EID (Security Issue?)
- Previously CREATED Objects Do Not Exist Which Will Trigger Deletion In EID (Data Destruction/User Impact)
- Members re-added (security issue?)/removed (loss of functionality?) from synched groups

- **THEREFORE:** Disable Connect Sync SCHEDULER Or Disable Cloud Sync CONFIGURATION BEFORE Forest Recovery!

- **DO NOT** Disable SYNC As A Feature In Entra ID !!!

# Authentication Mechanisms

> *Choose Wisely!*





# Risk/Impact Mitigating Actions

## > **CONNECT Sync**

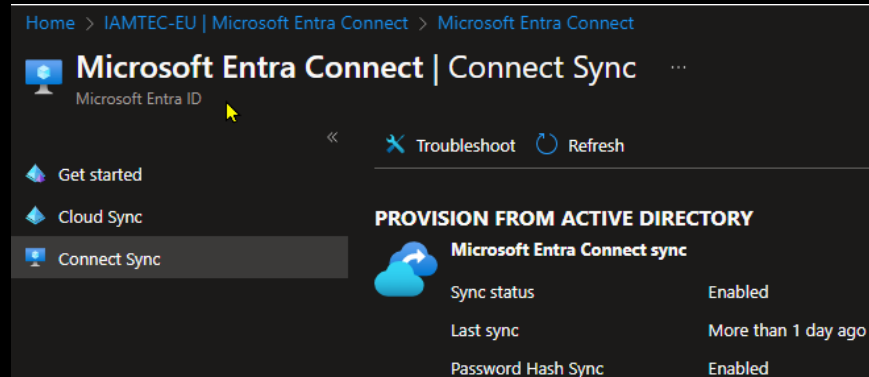
### When AD Is Down... (Synchronization)

#### ➤ **CONNECT Sync**

- Still Up-And-Running (i.e., NOT down/ransomwared)?
  - DISABLE The Connect Sync SCHEDULER

- Running Or Not...
  - DO NOT DISABLE Sync In EID!

```
Set-ADSyncScheduler -SyncCycleEnabled $false  
Get-ADSyncScheduler
```



Home > IAMTEC-EU | Microsoft Entra Connect > Microsoft Entra Connect

Microsoft Entra Connect | Connect Sync

Microsoft Entra ID

Get started

Cloud Sync

Connect Sync

Troubleshoot Refresh

**PROVISION FROM ACTIVE DIRECTORY**

**Microsoft Entra Connect sync**

Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled

# Risk/Impact Mitigating Actions

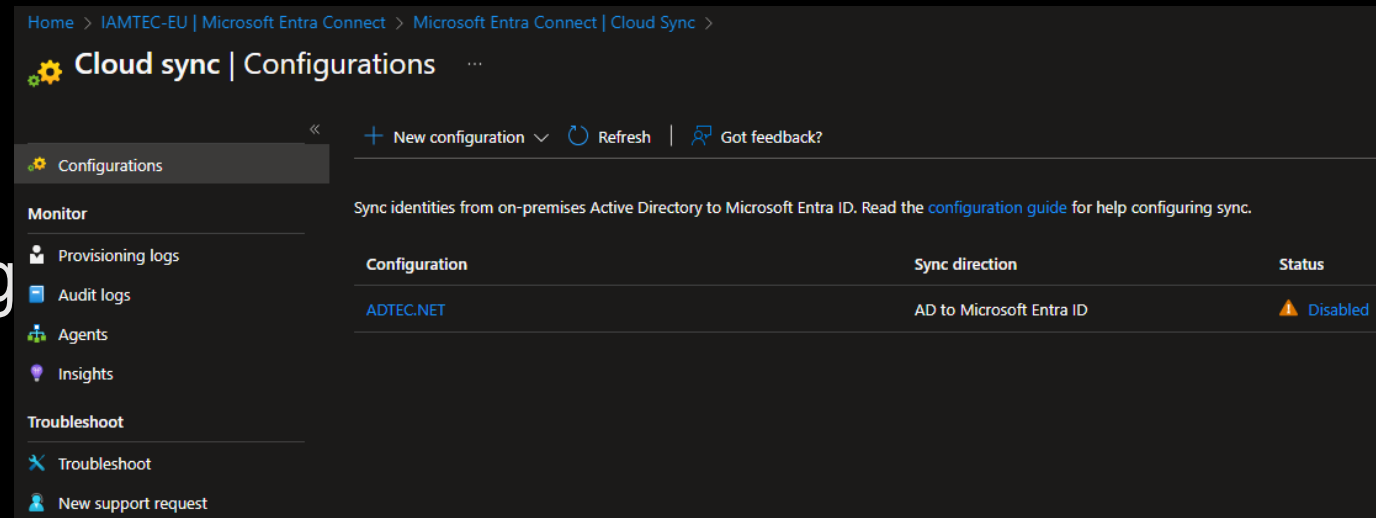
## > **CLOUD Sync**

### When AD Is Down... (Synchronization)

#### ➤ **CLOUD Sync**

- **DISABLE** The Cloud Sync Configuration In EID  
(Requires Global Admin Account)

- **DO NOT DELETE**  
Cloud Sync Config  
In EID!



Home > IAMTEC-EU | Microsoft Entra Connect > Microsoft Entra Connect | Cloud Sync >

### Cloud sync | Configurations

+ New configuration | Refresh | Got feedback?

Configurations

Monitor

- Provisioning logs
- Audit logs
- Agents
- Insights

Troubleshoot

- Troubleshoot
- New support request

Sync identities from on-premises Active Directory to Microsoft Entra ID. Read the [configuration guide](#) for help configuring sync.

Configuration	Sync direction	Status
ADTEC.NET	AD to Microsoft Entra ID	⚠ Disabled




# Risk/Impact Mitigating Actions

## > Authentication

### When AD Is Down... (Authentication)


- Native EID AuthN Through Password Hash Sync (PHS)
  - Nothing To Do Here!
  - AuthN Against EID Will Continue To Work!

**PROVISION FROM ACTIVE DIRECTORY**

 Azure AD Connect sync

Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled

**USER SIGN-IN**

 Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents
Email as alternate login ID	Disabled	

# Risk/Impact Mitigating Actions

## > Authentication

### When AD Is Down... (Authentication)

#### ➤ Pass-Through Authentication (PTA)

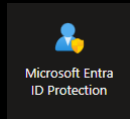
➤ No PHS As Backup? → THIS WILL HURT! 🤒

➤ PHS Enabled & Synched? → Disable PTA In AAD


➤ Download/Install PTA Agent ("[AADConnectAuthAgentSetup.exe](#)")

➤ Execute (Requires Global Admin Account):


```
CD "C:\Program Files\Microsoft Azure AD Connect Authentication Agent"
Import-Module ".\Modules\PassthroughAuthPSModule"
Get-PassthroughAuthenticationEnablementStatus
Disable-PassthroughAuthentication
Get-PassthroughAuthenticationEnablementStatus
```



#### PROVISION FROM ACTIVE DIRECTORY

	Azure AD Connect sync	
	Sync status	Enabled
	Last sync	More than 1 day ago
	Password Hash Sync	Enabled

#### USER SIGN-IN

	Federation	Disabled	0 domains
	Seamless single sign-on	Disabled	0 domains
	Pass-through authentication	Enabled	1 agent
	Email as alternate login ID	Disabled	

# Risk/Impact Mitigating Actions

## > Authentication

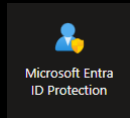
### When AD Is Down... (Authentication)

#### ➤ Federated AuthN Through ADFS/3<sup>rd</sup> Party Fed. System

➤ No PHS As Backup? → THIS WILL HURT!



➤ PHS Enabled/Synchd? → Convert Domain 2 Managed In EID (GA)



#### PROVISION FROM ACTIVE DIRECTORY



##### Azure AD Connect sync

Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled

#### USER SIGN-IN



Federation	Enabled	2 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Disabled	0 agents
Email as alternate login ID	Disabled	

```
Import-Module Microsoft.Graph.Identity.DirectoryManagement
Connect-MgGraph -TenantId <Tenant ID/FQDN> -Scopes "Domain.ReadWrite.All Directory.AccessAsUser.All"
$fedDomInEID = Get-MgDomain | ?{$_ .AuthenticationType -eq "Federated" -And $_.IsVerified -eq $true -And $_.IsRoot -eq $true}
$fedDomInEID | %{$domainId = $_.Id; $seid_Fed_CnfgPSObj = New-Object -TypeName PSObject; $seid_Fed_CnfgPSObj | Add-
Member -MemberType NoteProperty -Name DomainId -Value $domainId; $seid_Fed_Cnfg = Get-
MgDomainFederationConfiguration -DomainId $domainId; $seid_Fed_Cnfg | Get-Member | ?{$_ .MemberType -eq "Property"} |
%{$seid_Fed_CnfgPSObj | Add-Member -MemberType NoteProperty -Name $($_.Name) -Value $($seid_Fed_Cnfg.($_.Name))};
$seid_Fed_CnfgPSObj | Export-Clixml "eid_Fed_Cnfg_{$domainId}`_$((Get-Date -f "yyyyMMddHHmmss")).xml"
$fedDomInEID | %{Update-MgDomain -DomainId $($_.Id) -AuthenticationType Managed; Get-MgDomain -DomainId $($_.Id) | FL}
```



# Risk/Impact Mitigating Actions

## > Sync & Auth (Undoing)

### After Everything Is Back To “Normal” Again

- If Reconfigured, Revert Back To Previous AuthN Mechanism
  - PHS → PTA: Download/Install/Register PTA Agent
  - PHS → FED: Convert Domains From Managed 2 Federated

```
Import-Module Microsoft.Graph.Identity.DirectoryManagement
Connect-MgGraph -TenantId <Tenant ID/FQDN> -Scopes "Domain.ReadWrite.All Directory.AccessAsUser.All"
# PER PREVIOUSLY FEDERATED DOMAIN
$eid_Fed_CnfgHT = @{}; $eid_Fed_CnfgPSObj = Import-Clixml <Exported XML File>; $eid_Fed_CnfgPSObj | Get-Member | ?{$_ .MemberType -eq "NoteProperty"} | %{If (-not [string]::IsNullOrEmpty($eid_Fed_CnfgPSObj($_.Name)) -
And $_.Name -ne "Id" -And $_.Name -ne "SigningCertificateUpdateStatus" -And $eid_Fed_CnfgPSObj($_.Name).count-gt 0) {$eid_Fed_CnfgHT[($_.Name)] = $eid_Fed_CnfgPSObj($_.Name)}}
If (-not [string]::IsNullOrEmpty($eid_Fed_CnfgHT["FederatedIdpMfaBehavior"])) {New-MgDomainFederationConfiguration @eid_Fed_CnfgHT} Else {Write-Host "WARNING: Most Likely The Legacy 'SupportsMfa' Was Used And
Configured Previously. To Be Able To Change The Configuration Of The Domain, The Property 'FederatedIdpMfaBehavior' Must Be Configured In The Hash Table." -ForegroundColor Red}
Get-MgDomain -DomainId $eid_Fed_CnfgHT["DomainId"] | FL
Get-MgDomainFederationConfiguration -DomainId $eid_Fed_CnfgHT["DomainId"] | FL
```

**WARNING:** Pwd Changes In EID And Moving Back From PTA/Fed AuthN To Native AuthN?  
→ SSPR+WriteBack!



## What Is Being Used?

- Entra CONNECT Sync OR
- Entra CLOUD Sync

# Reconnecting Sync With Entra ID

**> For Starters**

## Assumed Starting Point

- AD Has Been Recovered
- AD Back To Production (Sync Down/Off!!!)
- “Fix” AD To Match Entra ID
- Connect Sync Server(s), Or Cloud Sync  
Prov. Agent(s) May Need To Be Fixed

# Reconnecting Sync With Entra ID

## > *Connect Sync Preparations*


### Connect Sync Down? → Need To Rebuild!

- Config/Rules Export Available?
- No Config Export?
  - OUs → Query Synched EID Objects Against AD & Create Unique List Of Parent Objects In Canonical Format!
-  Enabled Features? → “Tenant Sync Features”
-  Sign-In Methods? → “Tenant Sync Status” & Domain Configuration
- Sync Rules? → Hopefully Using Default, Otherwise Good Luck!

# Reconnecting Sync With Entra ID

## > *Connect Sync Preparations*

## Which Attribute For “Immutable ID”?

- When Down? → “Tenant Sync Config” 
- When Up? → Check Server Config AND Check Sync Rules With Join Criteria On AD And EID Side (Per Object Type!)

# Reconnecting Sync With Entra ID

## > *Connect Sync Preparations*

## Which Attribute For “Immutable ID”?

- AD “objectGuid” Attribute?
  - Upgrade To Latest Connect Version First (If Down: Install & Import Config, Same Version, Then Upgrade!)
  - Migrate 2 “ms-DS-ConsistencyGuid” Attrib
  - Using Fed.? → Update Claim Rules!
    - ADFS Managed Through Connect Wizard → Automatically
    - ADFS NOT Managed Through Connect Wiz. Or 3rd Party Fed → Fix Manually!
  - DO NOT Enable Sync At End Of Connect Wizard Configuration (Re)Configuration!



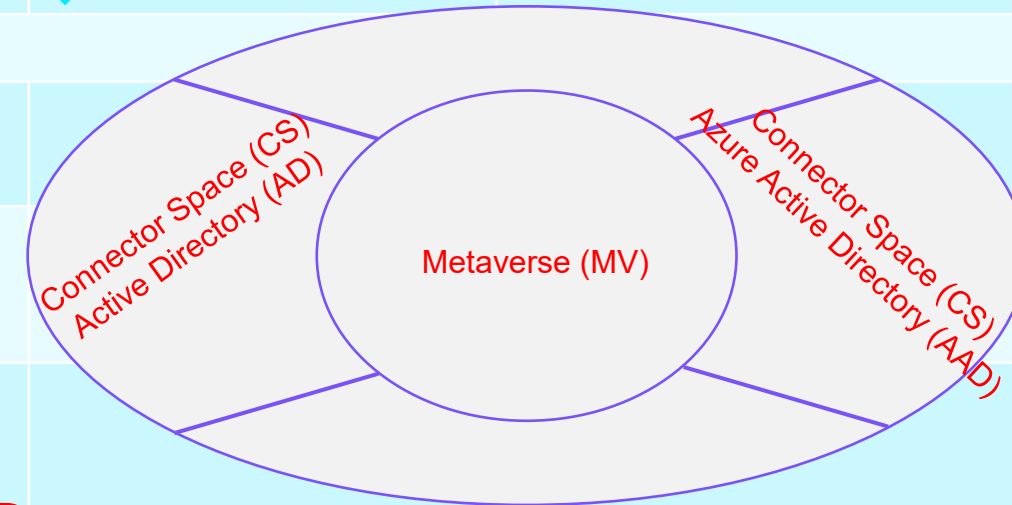
# Reconnecting Sync With Entra ID

## > Connect Sync Preparations



AD "USER" Objects + AD "INetOrgPerson" Objects  $\leftrightarrow$  AAD "USER" Objects

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
<b>JOIN RULES</b>				
<i>In From AD - XXX Join</i>	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
		sourceAnchor	sourceAnchor	<i>In from AAD - User Join</i>
<b>TRANSFORMATION(S)</b>				
<i>In From AD - XXX Join</i>	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
<i>In from AD - XXX AccountEnabled</i> <i>In from AD - XXX Common</i>	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
<i>In from AD - XXX AccountEnabled</i> <i>In from AD - XXX Common</i>	1) ms-DS-ConsistencyGuid (Base64) 2) objectGUID (Base64)	sourceAnchor		
<i>Out to AD - XXX ImmutableId</i>	ms-DS-ConsistencyGuid	sourceAnchorBinary		<i>← Rule/Flow IN-PLACE For USER Objects</i>
				<i>← Rule/Flow MISSING For INetOrgPerson Objects</i>
		1) userPrincipalName 2) accountName + %DomainFQDN%	onPremisesUserPrincipalName	<i>Out to AAD - User Join</i>





# Reconnecting Sync With Entra ID

## > Connect Sync Preparations



AD "GROUP" Objects  $\leftrightarrow$  AAD "GROUP" Objects

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
<b>JOIN RULES</b>				
<i>In From AD - Group Join</i>	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
		sourceAnchor	sourceAnchor	<i>In from AAD - Group Join</i>
<b>TRANSFORMATION(S)</b>				
<i>In From AD - Group Join</i>	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
<i>In from AD - Group Common</i>	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary		
<i>In from AD - Group Common</i>	1) ms-DS-ConsistencyGuid (Base64) 2) objectGUID (Base64)	sourceAnchor		
<i>Out to AD - Group ImmutableId</i>	ms-DS-ConsistencyGuid	sourceAnchorBinary		

← Rule/Flow MISSING





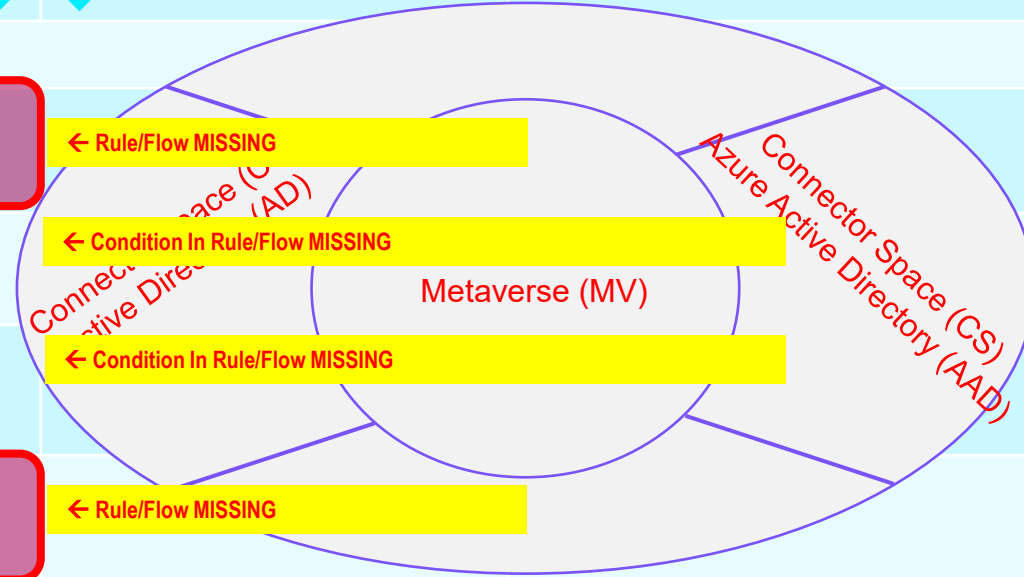
# Reconnecting Sync With Entra ID

## > Connect Sync Preparations



AD "CONTACT" Objects  $\leftrightarrow$  AAD "CONTACT" Objects

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
<b>JOIN RULES</b>				
In From AD - Contact Join	1) ms-DS-ConsistencyGuid 2) objectGUID Mail	sourceAnchorBinary Mail	← Join Condition In Rule MISSING	
		sourceAnchor	sourceAnchor	In from AAD - Contact Join
<b>TRANSFORMATION(S)</b>				
In From AD - Contact Join	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary	← Rule/Flow MISSING	
In from AD - Contact Common	1) ms-DS-ConsistencyGuid 2) objectGUID	sourceAnchorBinary	← Condition In Rule/Flow MISSING	
In from AD - Contact Common	1) ms-DS-ConsistencyGuid (Base64) 2) objectGUID (Base64)	sourceAnchor	← Condition In Rule/Flow MISSING	
Out to AD - Contact ImmutableId	ms-DS-ConsistencyGuid	sourceAnchorBinary	← Rule/Flow MISSING	





# Reconnecting Sync With Entra ID

## > Connect Sync Preparations



AD "COMPUTER" Objects  $\leftrightarrow$  AAD "DEVICE" Objects

Rule Name (AD)	CS AD Attribute(s)	MV Attribute	CS AAD Attribute	Rule Name (AAD)
<b>JOIN RULES</b>				
In from AD - Computer Join	1) ms-DS-ConsistencyGuid 2) objectGUID	deviceid	← Condition In Join Rule MISSING	
		deviceid	deviceid	In from AAD – Device Common
<b>TRANSFORMATION(S)</b>				
In from AD - Computer Join	<IIF Expression>	cloudFiltered	IIF Expression Updated To Only Flow When [ms-DS-ConsistencyGuid] = [objectGUID]	
	ObjectGUID	onPremisesObjectIdentifier	← Flow MISSING	
Out to AD - Computer ImmutableId	ms-DS-ConsistencyGuid	deviceid	← Rule/Flow MISSING	
<b>SCOPING FILTER(S)</b>				
	Condition REMOVED →	cloudCreated EQUAL false userCertificate ISNOTNULL cloudFiltered NOTEQUAL true		Out to AAD - Device Join SOAInAD

## GAP Analysis Between EID And AD

- Get Synched Objects From EID & Check Existence In AD (Using GC Of Correct AD!)
  - Multiple Forests Being Synched?

Object Type In AD	OnPremisesObjectIdentifier (EID) → ObjectGuid (AD)	OnPremiseSecurityIdentifier (EID) → ObjectSid (AD)
User/iNetOrgPerson	X	X
Group	X	X
Computer	X (Only When Flow Is Fixed)	X
Contact	X	

# Reconnecting Sync With Entra ID

## > Finding The GAPS

- Using “OnPremiseSecurityIdentifier (EID)” Against ObjectSid (AD) Is Preferred! (Where Possible)

# Reconnecting Sync With Entra ID

> *Closing The GAPS*



## Fixing Objects In AD Using Data From EID

- Recreate MISSING Users/iNetOrgPersons, Groups, Contacts In AD
  - Domain/OU To Create Object In?
  - Populate Attributes Known To AAD (e.g. UPN, sAMAccountName, etc.)
  - Populate The “Immutable ID” Value
  - Get (New) objectGuid/objectSid
  - Enrich With Data From IAM System!
- NOTE: Cleanup Excess Objects As Needed (Optional) (And Tricky And Tough To Do!)

# Reconnecting Sync With Entra ID

> *Closing The GAPS*

## Fixing Objects In AD Using Data From EID

- Fix Relationships (e.g. Memberships) In AD
  - Relationship Information Needs To Be Translated From AAD To AD!
    - MSFT Graph API (objectId)
    - DirSync API (ImmutableId)
    - AD (distinguishedName)  
(Look It Up Using ACTIVE  
objectGuid/objectSid)
  - Just Re-Add All Members
  - Removing Excess Members (Tricky!)

# Reconnecting Sync With Entra ID

**> Uniqueness Of Objects**

## Getting “Immutable ID” Values



- MSFT (MSOL, AAD, Graph) PoSH And “Immutable ID”:
  - Exposed For Users
  - NOT Exposed For Groups
  - NOT Exposed For Computers
  - NOT Exposed For Contacts



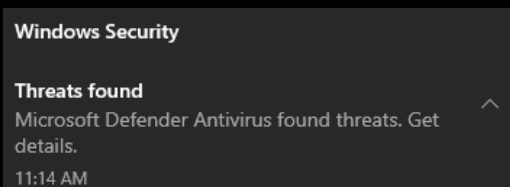
# Reconnecting Sync With Entra ID

## > Uniqueness Of Objects

## Getting “Immutable ID” Values

- Connect Sync And “Immutable ID”:
  - Query AAD Connector Space (If Available, Might Be Outdated/Incomplete)
  -  ➤ Query DirSync API Through AADInternals PoSH Module (= Non-MSFT!)
  - Using Cloud Sync?
    -  ➤ Query DirSync API Through AADInternals PoSH Module (= Non-MSFT!)

## Downside Of AAD Internals POSH Module?



```
PS C:\Users\Administrator> Install-Module AADINTERNALS -Force
PackageManagement\Install-Package : Package 'AADInternals' failed to be installed because: Operation did not complete successfully
because the file contains a virus or potentially unwanted software.
At C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1:1809 char:21
+ ...          $null = PackageManagement\Install-Package @PSBoundParameters
+ ~~~~~
+ CategoryInfo          : InvalidResult: (AADInternals:String) [Install-Package], Exception
+ FullyQualifiedErrorId : Package '{0}' failed to be installed because: {1},Microsoft.PowerShell.PackageManagement.Cmdlets.InstallPackage
```



# Reconnecting Sync With Entra ID

## > *Reenabling (CONNECT) Sync*

- Manual Full Import On AD Connector
- Manual Full Import On AAD Connector
- Can Be Done In Parallel
  - Only Applies To IMPORT/EXPORT!
  - DOES NOT Apply To SYNC!



# Reconnecting Sync With Entra ID

## > Reenabling (CONNECT) Sync

DO NOT SYNC ONLY

Objects And 10 (?)

Preview

Contents

- Start Preview
- Source Object Details
- Import Attribute Flow
- Connector Updates
  - CN=usrAADConSyncR001,OU=AA
    - Export Attribute Flow**
  - CN={4C35536C6B482F7A7A30436
    - Export Attribute Flow

Export Attribute Flow

Export flow mode: **full**

Sync Rule	Data Source	Mapping Type	Data Source Attribute	Initial Value	Final Value
	<Unavailable>	<System>	cn	usrAADConSync...	(Unchanged)
	<Unavailable>	<System>	countryCode	0	(Unchanged)

Preview

Contents

- Start Preview
- Source Object Details
- Import Attribute Flow
- Connector Updates
  - CN=usrAADConSyncR001,OU=AA
    - Export Attribute Flow
  - CN={4C35536C6B482F7A7A30436
    - Export Attribute Flow**

Out to AD - Us...

Export Attribute Flow

Export flow mode: **full**

Sync Rule	Data Source	Mapping Type	Data Source Attribute	Initial Value	Final Value
Out to AAD - U...	accountEnabled	Direct	accountEnabled	true	(Unchanged)
	<Unavailable>	<System>	cloudAnchor	User_51561630f...	(Unchanged)
	<Unavailable>	<System>	cloudMastered	false	(Unchanged)
Out to AAD - U...	cn	Direct	commonName	usrAADConSync...	(Unchanged)
Out to AAD - U...	IIF(IsNullOrEmpty([count...	Expression	countryCode	0	(Unchanged)
Out to AAD - U...	description	Direct	description	NEW	(Unchanged)
Out to AAD - U...	displayName	Direct	displayName	usrAADConSync...	(Unchanged)
Out to AAD - U...	domainFQDN	Direct	dnsDomainName	ADTEC.NET	(Unchanged)
Out to AAD - U...	extension_mS-DS-Consi...	Direct	extension_ba1d29762a...	2F 94 A5 90 7F F...	(Unchanged)
Out to AAD - U...	extension_objectGUID	Direct	extension_ba1d29762a...	2F 94 A5 90 7F F...	(Unchanged)
Out to AAD - U...	givenName	Direct	givenName	usrAADConSync...	(Unchanged)
Out to AAD - U...	pwdLastSet	Direct	lastPasswordChange Ti...	20230224103720...	(Unchanged)
Out to AAD - U...	domainNetBios	Direct	netBiosName	ADTEC	(Unchanged)
Out to AAD - U...	objectSid	Direct	onPremiseSecurityIdenti...	01 05 00 00 00 0...	(Unchanged)
Out to AAD - U...	distinguishedName	Direct	onPremisesDistinguishe...	CN=usrAADConS...	(Unchanged)
Out to AAD - U...	accountName	Direct	onPremisesSamAccoun...	usrAADConSync...	(Unchanged)
Out to AAD - U...	IIF(IsPresent([cloudSour...	Expression	sourceAnchor	L5SikH/zz0Cb6y...	(Unchanged)
Out to AAD - U...	sn	Direct	sumame	usrAADConSync...	(Unchanged)
Out to AAD - U...	title	Direct	title	NEW	(Unchanged)
Out to AAD - U...	userPrincipalName	Direct	userPrincipalName	usrAADConSync...	(Unchanged)
Out to AAD - U...	"CN={" & ConvertToUT...	Expression	dn		CN={4C35536C...

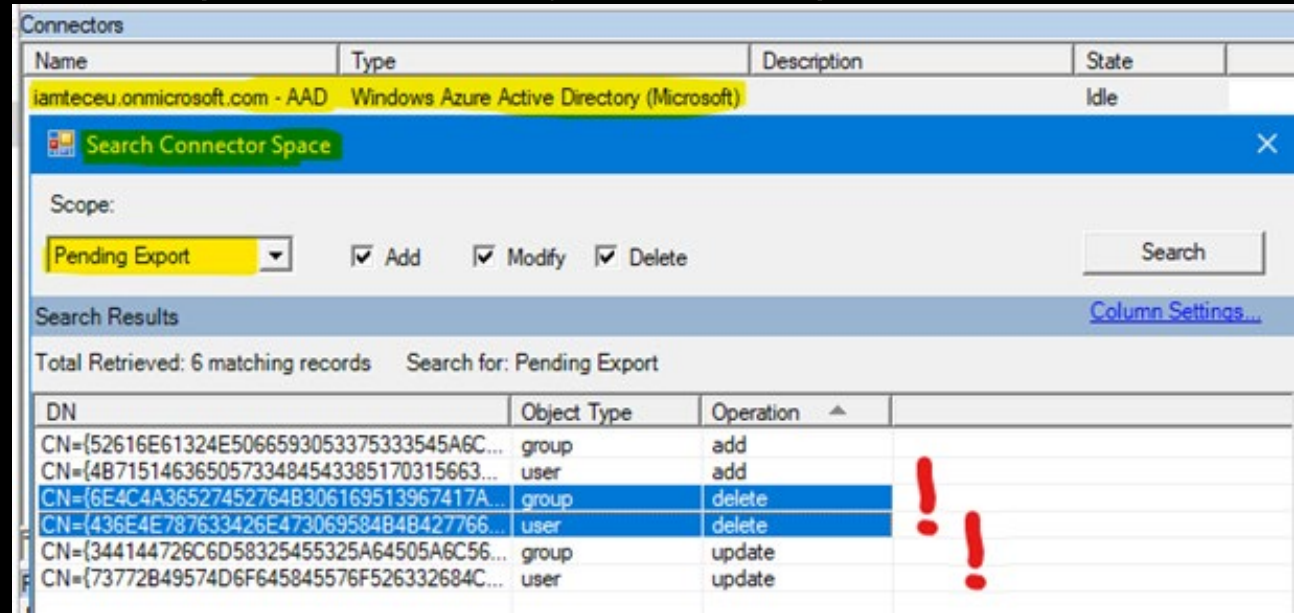
➤ DO NOT EX

# Reconnecting Sync With Entra ID

> **Reenabling (CONNECT)  
Sync**

## Starting The Checks - Manually

- Manual Full Synchronization On AD Connector
- On AAD Connector, Evaluate Pending Exports (Add, Modify, Delete)



Name	Type	Description	State
iamteceu.onmicrosoft.com - AAD	Windows Azure Active Directory (Microsoft)		Idle

Search Connector Space

Scope: Pending Export

Add  Modify  Delete

Search

Search Results

Total Retrieved: 6 matching records Search for: Pending Export

DN	Object Type	Operation
CN={52616E61324E5066593053375333545A6C...}	group	add
CN={4B71514636505733484543385170315663...}	user	add
CN={6E4C4A36527452764B306169513967417A...}	group	delete
CN={436E4E787633426E473069584B4B427766...}	user	delete
CN={344144726C6D58325455325A64505A6C56...}	group	update
CN={73772B49574D6F645845576F526332684C...}	user	update

# Reconnecting Sync With Entra ID

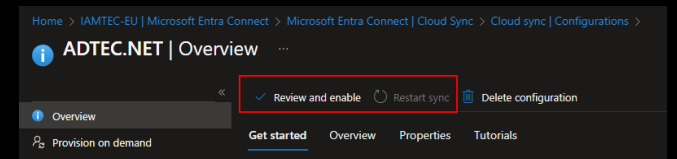
> **Reenabling (CLOUD)  
Sync**

## Starting The Checks - Manually

- You Can't! (Remember: On/Off Only!)

## Enable ~~Controlled Manual~~ Sync

- For EACH Cloud Sync Configuration
  - Reconfigure Deletion Threshold To 1
  - (Re-)Enable Configuration
  - Restart Sync



- Be Patient...

- ...AND PRAY ALL IS OK!



# Reconnecting Sync With Entra ID

## > Reenabling (CLOUD) Sync

Unfortunately, IT IS NOT Going To Be OK!

➤ Behavioral Di (High-Level!)



➤ Connect  
Existing

➤ Backup Cloud Sync Configuration(s)  
➤ Delete Cloud Sync Configuration(s)

Connect To  
Object



➤ Cloud S  
Object, I  
Deleted

➤ Restore Cloud Sync Configuration(s)  
➤ Disable Cloud Sync Configuration(s)  
➤ Configure Deletion Threshold To 1

ce Of AD  
Object To

**END  
RESULT**

➤ S  
➤ Synced Groups, Contacts, Computers. Hard-Delete > Recreated

➤ Enable Cloud Sync Configuration(s)  
➤ Restart Sync Per Cloud Sync Configuration

d > Updated  
Recreated





# Reconnecting Sync With Entra ID

## > *Reenabling (CLOUD) Sync*

BEFORE Re-Enabling (Connect/Cloud) Sync...

- Check Entra Users Audit Logs (Category=UserManagement) For
  - Date = Max 30 Days Ago
  - Activity = Change Password (Self-Service)
  - Activity = Change User Password
  - Activity = Reset Password (By Admin)
  - Activity = Reset Password (Self-Service)
  - Activity = Reset User Password



# Reconnecting Sync With Entra ID

## > *Reenabling (CLOUD) Sync*

When Re-Enabling (Connect/Cloud) Sync...

- DO NOT Re-Enable PHS
- Use SSPR+WriteBack To Get Passwords In Sync Again Between AD And EID
- Then Re-Enable PHS

# Take Aways

## > Recommendations

## The DR Plan → Bus. Continuity Plan (BCP)

- Be Prepared! Things In Place Save



- Not AD Only! Include EVERYTHING Depending On Or Related To AD (e.g. ADFS, ADCS, Entra Connect/Cloud Sync, etc.)
- Also Include (Required):
  - Possible/Immediate Pre-Actions (e.g. Impact/Risk-Mitigation)
  - Post-Actions (e.g. Improve Security, GAP Analysis)

## Entra ID Authentication

- Make Sure To Have PHS As Primary Or Backup!
- As Backup? → Be Prepared To Change/Convert

## Take Aways

### > *Recommendations*

### For Entra CONNECT Only

- Still Using “ObjectGUID”? → “Migrate To “ms-DS-ConsistencyGuid” As Immutable ID, A.S.A.P.!”
- Fix And Update Sync Rules



# Choosing Between Connect Sync And Cloud Sync

➤ Opinions And Millage May Vary, But...

## Take Aways

> **Recommendations**

### Backups/Exports

➤ In Addition To AD Backups, Regularly Export & Secure Config(s) of Connect Sync, Cloud Sync, ADFS, ADCS, “Others” As Applicable

**!! AUTOMATE – AUTOMATE – AUTOMATE !!**



SCAN ME

<b>Jorge de Almeida Pinto</b> Senior Incident Response Lead	
<b>LinkedIn</b>	<a href="http://tiny.cc/JorgeLinkedIn">http://tiny.cc/JorgeLinkedIn</a>
<b>Blog</b>	<a href="http://tiny.cc/JQFKblog">http://tiny.cc/JQFKblog</a>
<b>Twitter</b>	<a href="http://tiny.cc/JQFKtwitter">http://tiny.cc/JQFKtwitter</a>
<b>Website</b>	<a href="https://www.semperis.com/">https://www.semperis.com/</a>
<b>Blog</b>	<a href="https://www.semperis.com/blog/">https://www.semperis.com/blog/</a>
<b>Podcast</b>	<a href="https://hipconf.libsyn.com/">https://hipconf.libsyn.com/</a>
<b>Contact</b>	<a href="mailto:jorged@semperis.com">jorged@semperis.com</a>



Questions? 