# Identity Awareness

Expected Time: 1 Hour

## Introduction

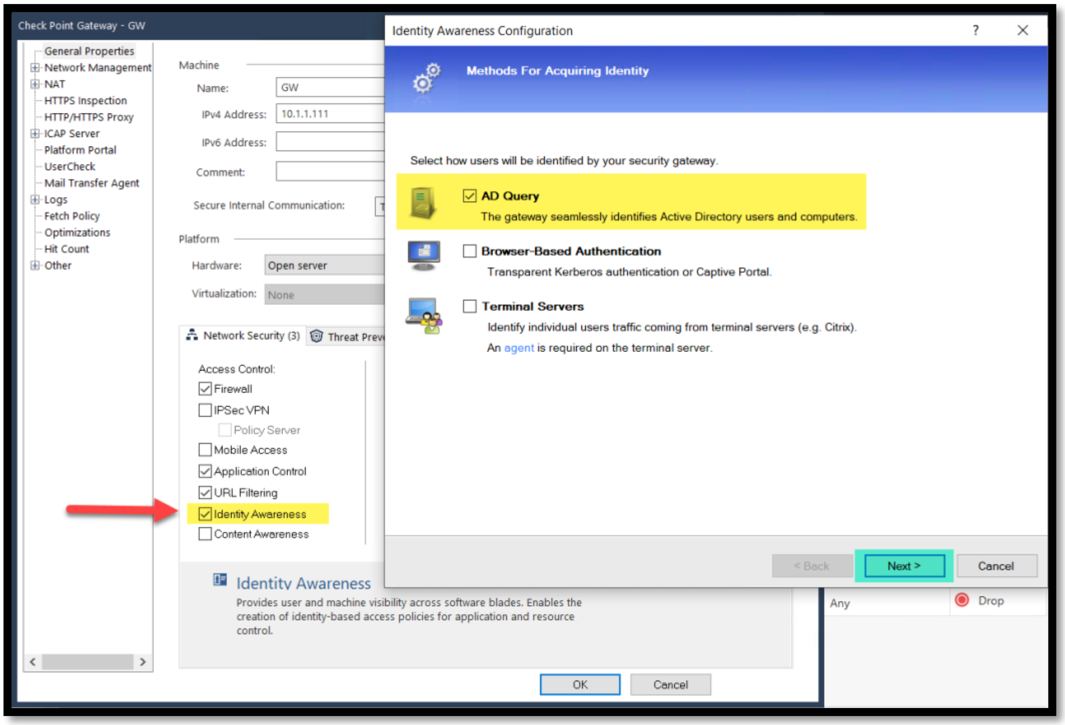
Check Point Identity Awareness offers granular visibility of users, groups, and machines, providing unmatched application and access control through the creation of accurate, identity-based policies.

Centralized management and monitoring allow for policies to be managed from a single, unified console.

## Exercise 1: ADQuery

**AD Query** is an easy to configure, clientless tool to get identities. Its function is based on Active Directory integration, and it is fully transparent to the user.

1. Edit the GW object and enable the Identity Awareness blade. Leave AD Query and continue to the next step.



Machine
Name: GW
IPv4 Address: 10.1.1.111
IPv6 Address:
Comment:
Secure Internal Communication:

Platform
Hardware: Open server
Virtualization: None

Access Control:
☑ Firewall
☐ IPSec VPN
☐ Policy Server
☐ Mobile Access
☑ Application Control
☑ URL Filtering
☑ Identity Awareness
☐ Content Awareness

Identity Awareness
Provides user and machine visibility across software blades. Enables the creation of identity-based access policies for application and resource control.

Select how users will be identified by your security gateway.

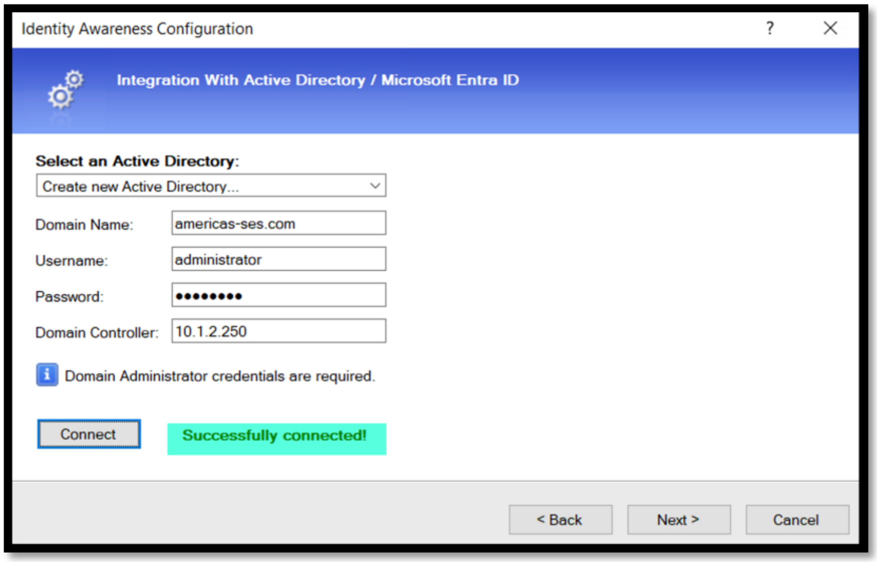
☑ **AD Query**
The gateway seamlessly identifies Active Directory users and computers.

☐ **Browser-Based Authentication**
Transparent Kerberos authentication or Captive Portal.

☐ **Terminal Servers**
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An agent is required on the terminal server.

2. Fill in the required Active Directory details and click **Connect**. Make sure the connection is successful and finish the configuration wizard and close the GW object.

| | |
|---|---|
| **Domain Name** | **americas-ses.com** |
| **Username** | administrator |
| **Password** | Cpwins!1 |
| **Domain Controller** | 10.1.2.250 |


Identity Awareness Configuration

Integration With Active Directory / Microsoft Entra ID

Select an Active Directory: Create new Active Directory...

Domain Name: americas-ses.com

Username: administrator

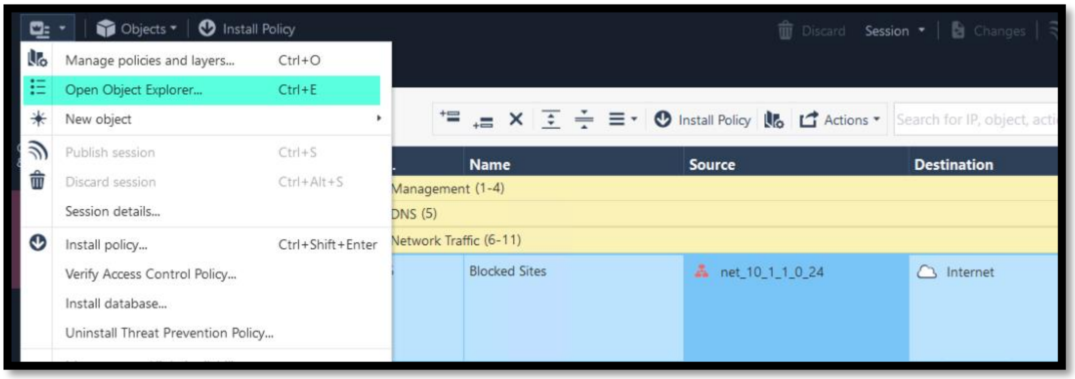
Password: ••••••••

Domain Controller: 10.1.2.250

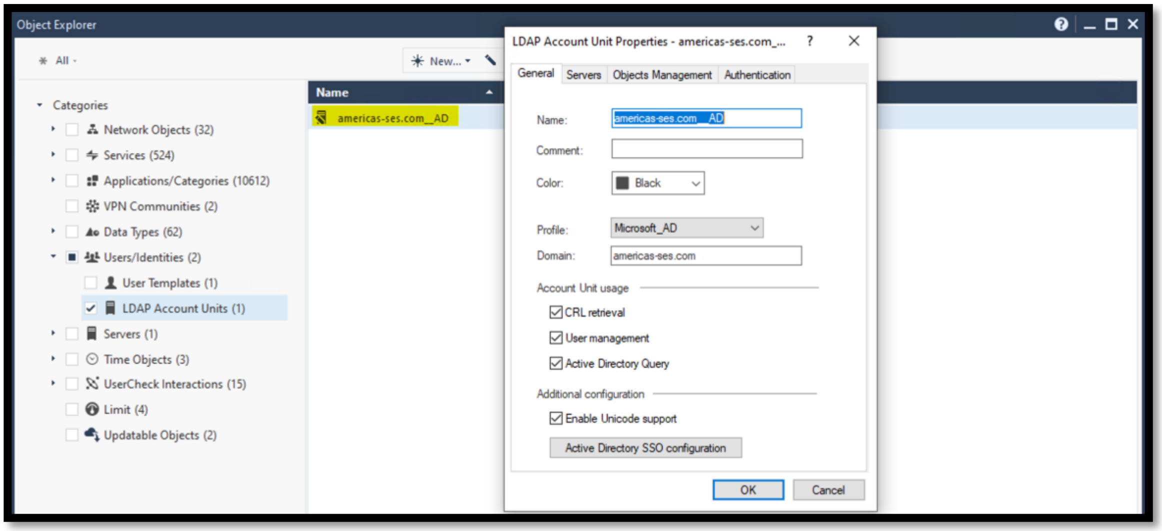
Domain Administrator credentials are required.

Successfully connected!

3. The wizard above creates an Account unit object. This object contains all configurations related the active directory. Open the Object Explorer.



4. Navigate to the **LDAP Account Units** and review the configured settings on the automatically created object and close the window.



Name: americas-ses.com__AD

Comment:

Color: Black

Profile: Microsoft_AD

Domain: americas-ses.com

Account Unit usage

☑ CRL retrieval

☑ User management

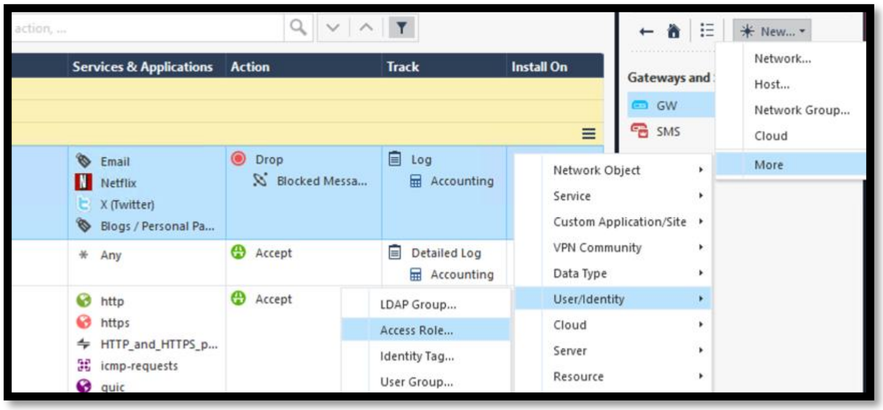
☑ Active Directory Query

Additional configuration

☑ Enable Unicode support

5. Publish the current Session.

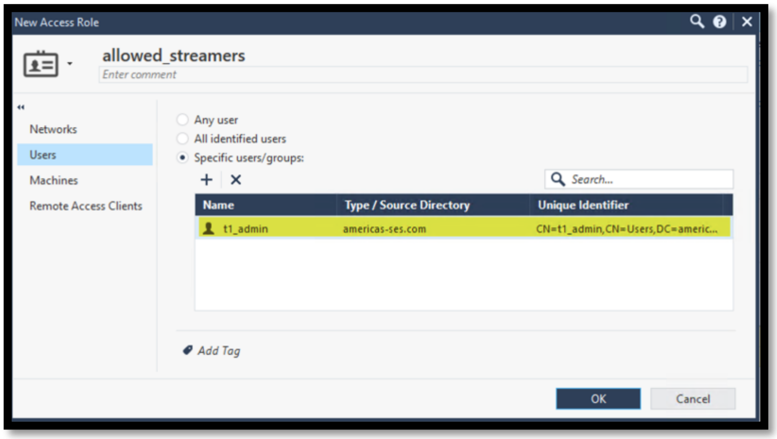
6. Create a new Access Role **New** -> **More** -> **User/Identity** -> **Access Role**.



- You can use **Access Role** objects as source and/or destination parameter in a rule. Access Role objects can include one or more of these objects:
    - Networks
    - Users and user groups
    - Computers and computer groups
    - Remote Access clients

7. We will create rules to block all media streaming applications and allow it to one specific group of users. Give the object a proper name. E.g. **allowed_streamers**.

8. Select the **Users** - > **Specific users/groups** and add the **t1_admin** user and click Ok and close the Object.



New Access Role

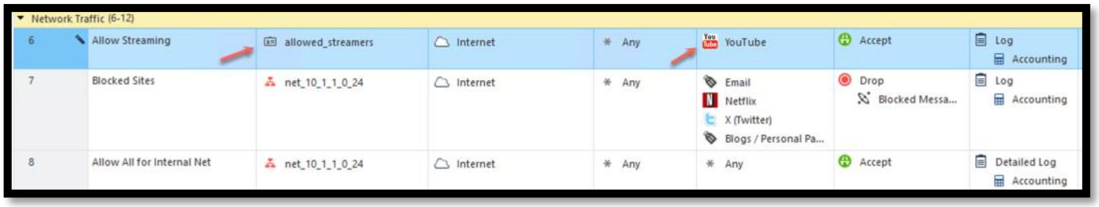
allowed_streamers

Enter comment

○ Any user
○ All identified users
● Specific users/groups:

| Name | Type / Source Directory | Unique Identifier |
|---|---|---|
| t1_admin | americas-ses.com | CN=t1_admin,CN=Users,DC=americ... |

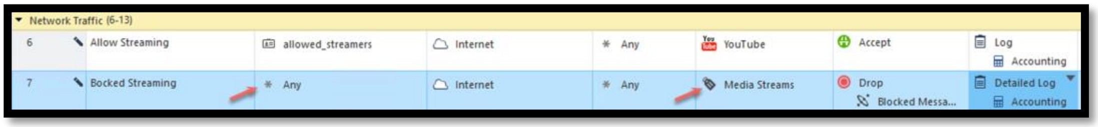
9. Create a new rule on top of the **Blocked Sites** rule. This rule allows the users from the Access Role we created in the previous step. **t1_admin** is allowed to access **YouTube**.



Network Traffic (6-12)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | Allow Streaming | allowed_streamers | Internet | Any | YouTube | Accept | Log<br>Accounting |
| 7 | Blocked Sites | net_10_1_1_0_24 | Internet | Any | Email<br>Netflix<br>X (Twitter)<br>Blogs / Personal Pa... | Drop<br>Blocked Messa... | Log<br>Accounting |
| 8 | Allow All for Internal Net | net_10_1_1_0_24 | Internet | Any | Any | Accept | Detailed Log<br>Accounting |

10. Add a rule below it will Drop traffic from **Any** source to all **Media Steaming** sites including **YouTube**.

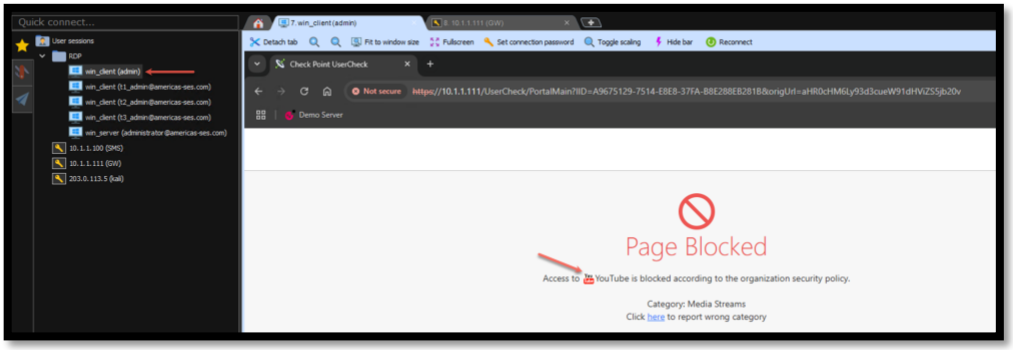


Network Traffic (6-13)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | Allow Streaming | allowed_streamers | Internet | Any | YouTube | Accept | Log<br>Accounting |
| 7 | Bocked Streaming | Any | Internet | Any | Media Streams | Drop<br>Blocked Messa... | Detailed Log<br>Accounting |

11. **Install the access policy**. *This is required before we can pull objects from the AD server*.

12. Login to the **win_client** host and test reaching **YouTube**. It should be blocked based on **Rule 7** because the saved RDP session is using the local *(non -AD account)* account **admin.**



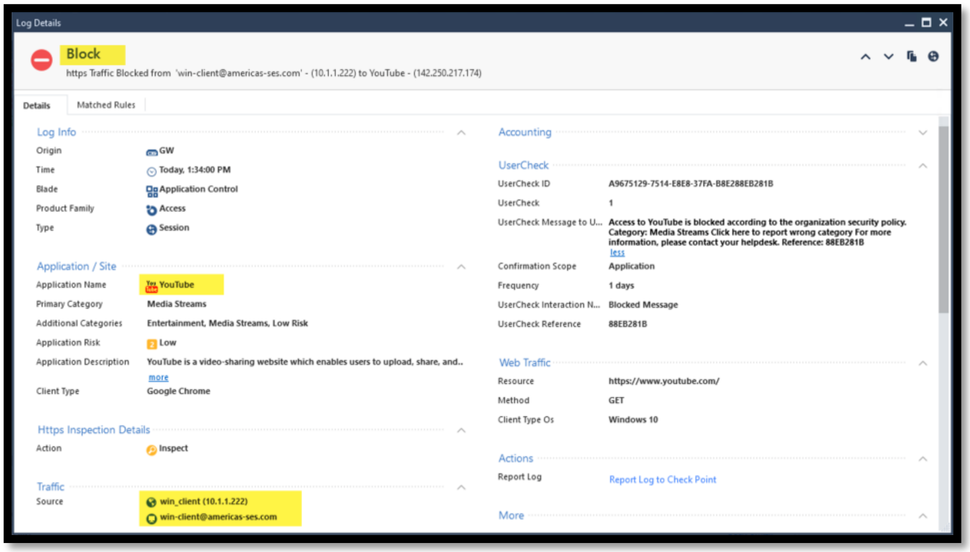
https://10.1.1.111/UserCheck/PortalMain?IID=A9675129-7514-E8E8-37FA-B8E288EB281B&origUrl=aHR0cHM6Ly93d3cueW91dHViZS5jb20v

Page Blocked

Access to YouTube is blocked according to the organization security policy.

Category: Media Streams
Click here to report wrong category

13. Review the logs and confirm that the traffic was blocked by the correct rule.



Log Details

**Block**

https Traffic Blocked from 'win-client@americas-ses.com' - (10.1.1.222) to YouTube - (142.250.217.174)

Details | Matched Rules

**Log Info**

| | |
|---|---|
| Origin | GW |
| Time | Today, 1:34:00 PM |
| Blade | Application Control |
| Product Family | Access |
| Type | Session |

**Application / Site**

| | |
|---|---|
| Application Name | YouTube |
| Primary Category | Media Streams |
| Additional Categories | Entertainment, Media Streams, Low Risk |
| Application Risk | 2 Low |
| Application Description | YouTube is a video-sharing website which enables users to upload, share, and..<br>more |
| Client Type | Google Chrome |

**Https Inspection Details**

| | |
|---|---|
| Action | Inspect |

**Traffic**

| | |
|---|---|
| Source | win_client (10.1.1.222)<br>win-client@americas-ses.com |

**Accounting**

**UserCheck**

| | |
|---|---|
| UserCheck ID | A9675129-7514-E8E8-37FA-B8E288EB281B |
| UserCheck | 1 |
| UserCheck Message to U... | Access to YouTube is blocked according to the organization security policy. Category: Media Streams Click here to report wrong category For more information, please contact your helpdesk. Reference: 88EB281B<br>less |
| Confirmation Scope | Application |
| Frequency | 1 days |
| UserCheck Interaction N... | Blocked Message |
| UserCheck Reference | 88EB281B |

**Web Traffic**

| | |
|---|---|
| Resource | https://www.youtube.com/ |
| Method | GET |
| Client Type Os | Windows 10 |

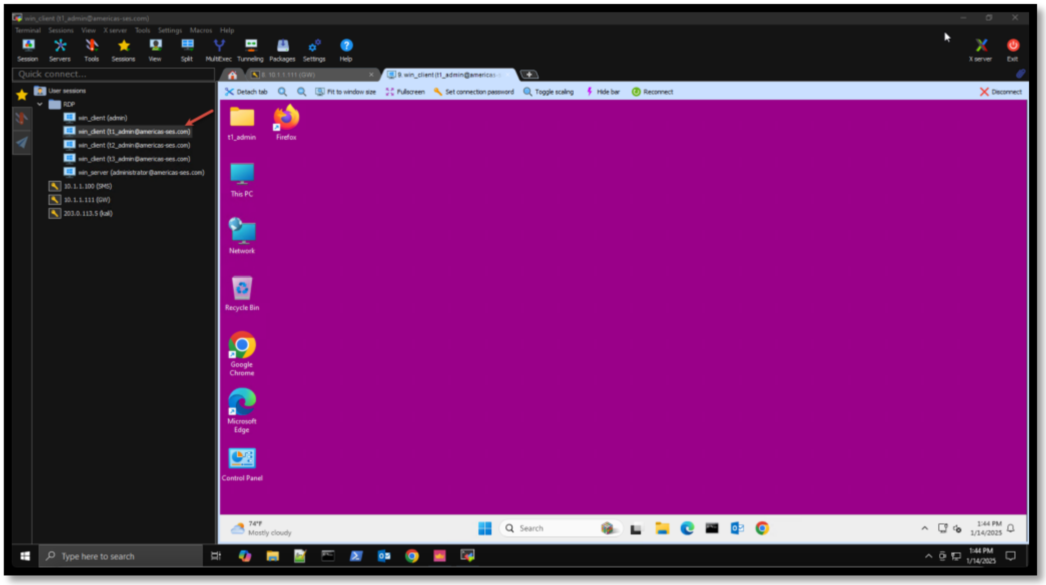
**Actions**

| | |
|---|---|
| Report Log | Report Log to Check Point |

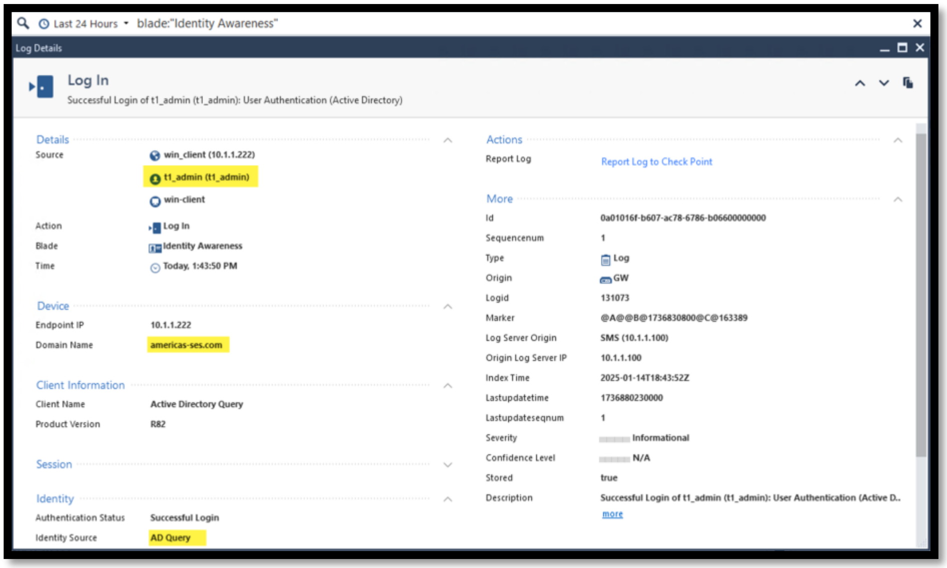
**More**

14. Login to the same host **win_client** as **t1_admin/Cpwins!1.** The session is saved in the same client.

- Note that this user is part of the access rule we created earlier, and it is allowed to reach **YouTube**.
- The machine below is part of the domain (Americas-ses.com). The login will create an event which will be forwarded to the GW. The GW will associate the identity of user t1_admin to the host 10.1.1.222 (windows-client).


win_client (t1_admin@americas-ses.com)
Terminal Sessions View X server Tools Settings Macros Help
Session Servers Tools Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
8. 10.1.1.111 (GW)
9. win_client (t1_admin@americas-s
Detach tab Fit to window size Fullscreen Set connection password Toggle scaling Hide bar Reconnect Disconnect
User sessions
RDP
win_client (admin)
win_client (t1_admin@americas-ses.com)
win_client (t2_admin@americas-ses.com)
win_client (t3_admin@americas-ses.com)
win_server (administrator@americas-ses.com)
10.1.1.100 (SMS)
10.1.1.111 (GW)
203.0.113.5 (kali)
t1_admin
Firefox
This PC
Network
Recycle Bin
Google Chrome
Microsoft Edge
Control Panel
74°F Mostly cloudy
Search
1:44 PM 1/14/2025
Type here to search

15. Filter the logs to see Identity Awareness related logs. Notice that the user identity was acquired correctly and that the Access Role was associated to this user.



Last 24 Hours blade:"Identity Awareness"

Log Details

Log In

Successful Login of t1_admin (t1_admin): User Authentication (Active Directory)

Details

| | |
|---|---|
| Source | win_client (10.1.1.222)<br>t1_admin (t1_admin)<br>win-client |
| Action | Log In |
| Blade | Identity Awareness |
| Time | Today, 1:43:50 PM |

Device

| | |
|---|---|
| Endpoint IP | 10.1.1.222 |
| Domain Name | americas-ses.com |

Client Information

| | |
|---|---|
| Client Name | Active Directory Query |
| Product Version | R82 |

Session

Identity

| | |
|---|---|
| Authentication Status | Successful Login |
| Identity Source | AD Query |

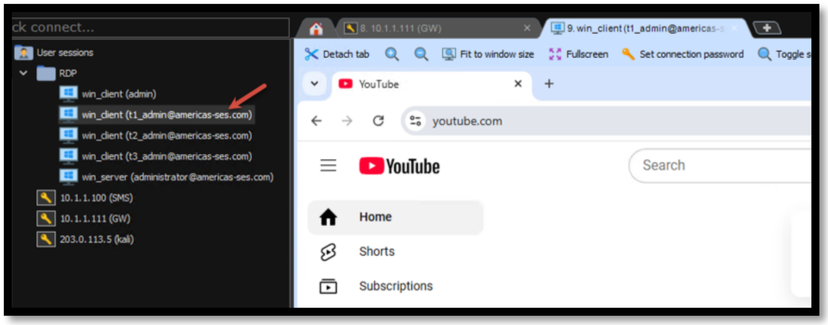
Actions

| | |
|---|---|
| Report Log | Report Log to Check Point |

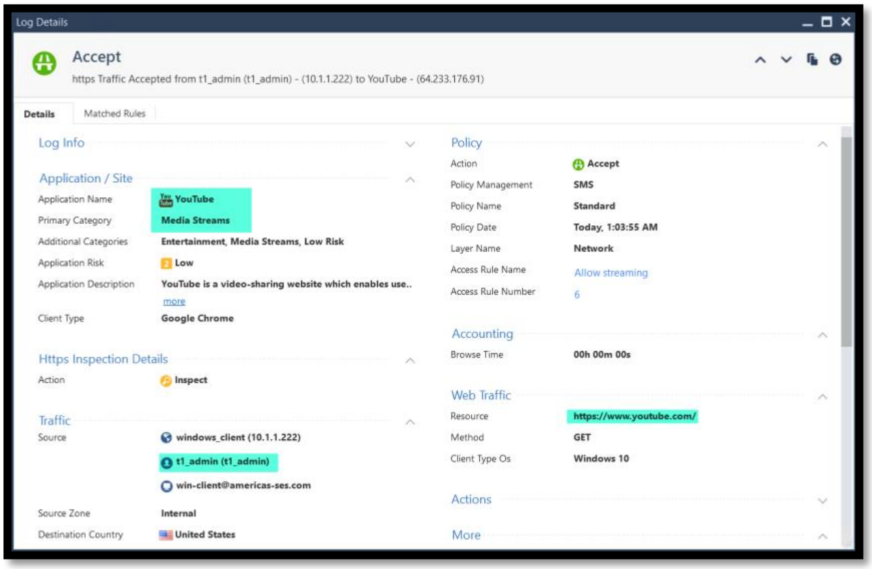
More

| | |
|---|---|
| Id | 0a01016f-b607-ac78-6786-b06600000000 |
| Sequencenum | 1 |
| Type | Log |
| Origin | GW |
| Logid | 131073 |
| Marker | @A@@B@1736830800@C@163389 |
| Log Server Origin | SMS (10.1.1.100) |
| Origin Log Server IP | 10.1.1.100 |
| Index Time | 2025-01-14T18:43:52Z |
| Lastupdatetime | 1736880230000 |
| Lastupdateseqnum | 1 |
| Severity | Informational |
| Confidence Level | N/A |
| Stored | true |
| Description | Successful Login of t1_admin (t1_admin): User Authentication (Active D..<br>more |

16. Try to reach YouTube. It should be allowed by rule 6 as this user is part of the **allowed_streamers** access role.



17. Review the Application control logs and confirm that the traffic was allowed by the correct rule.



Log Details

Accept

https Traffic Accepted from t1_admin (t1_admin) - (10.1.1.222) to YouTube - (64.233.176.91)

Details | Matched Rules

Log Info

Application / Site

| | |
|---|---|
| Application Name | YouTube |
| Primary Category | Media Streams |
| Additional Categories | Entertainment, Media Streams, Low Risk |
| Application Risk | 2 Low |
| Application Description | YouTube is a video-sharing website which enables use..<br>more |
| Client Type | Google Chrome |

Https Inspection Details

| | |
|---|---|
| Action | Inspect |

Traffic

| | |
|---|---|
| Source | windows_client (10.1.1.222)<br>t1_admin (t1_admin)<br>win-client@americas-ses.com |
| Source Zone | Internal |
| Destination Country | United States |

Policy

| | |
|---|---|
| Action | Accept |
| Policy Management | SMS |
| Policy Name | Standard |
| Policy Date | Today, 1:03:55 AM |
| Layer Name | Network |
| Access Rule Name | Allow streaming |
| Access Rule Number | 6 |

Accounting

| | |
|---|---|
| Browse Time | 00h 00m 00s |

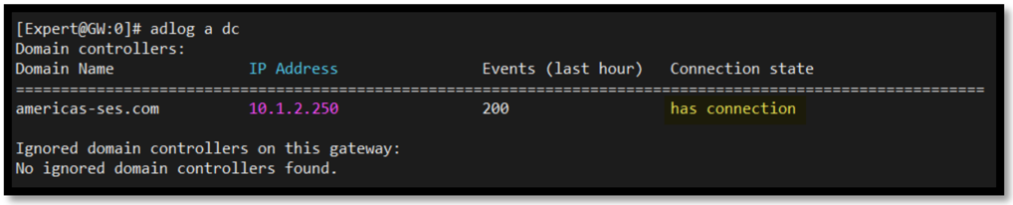
Web Traffic

| | |
|---|---|
| Resource | https://www.youtube.com/ |
| Method | GET |
| Client Type Os | Windows 10 |

Actions

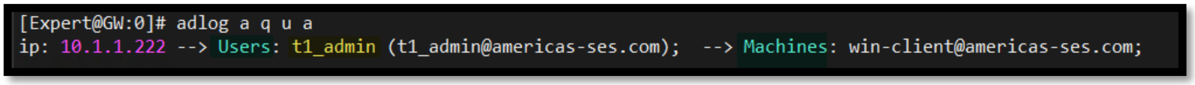
More

18. Login to the GW over ssh and run the command **adlog a dc** to see the connected domains, domain controllers and their status.



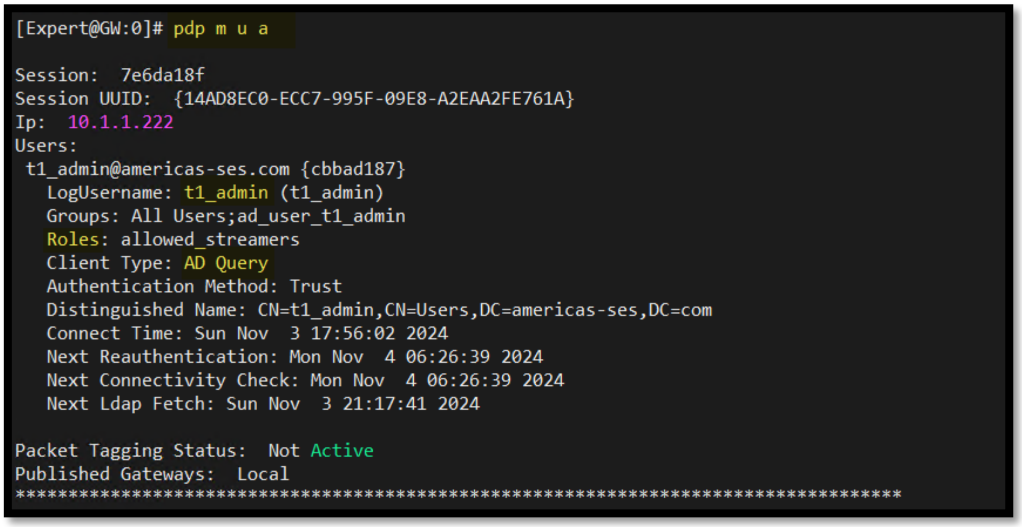
```
[Expert@GW:0]# adlog a dc
Domain controllers:
Domain Name             IP Address             Events (last hour)   Connection state
==================================================================================================
americas-ses.com        10.1.2.250             200                  has connection

Ignored domain controllers on this gateway:
No ignored domain controllers found.
```

19. To see all discovered identities based on the AD events, run the command **adlog a q u a**.



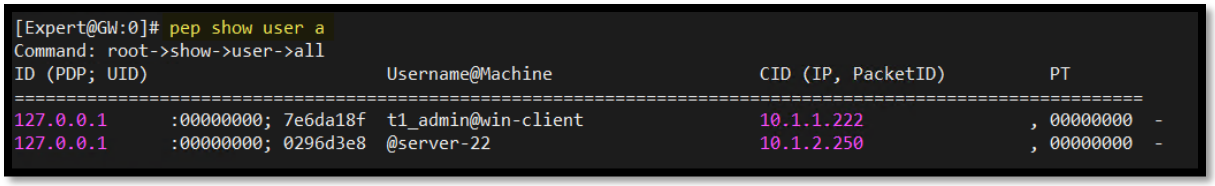
```
[Expert@GW:0]# adlog a q u a
ip: 10.1.1.222 --> Users: t1_admin (t1_admin@americas-ses.com);  --> Machines: win-client@americas-ses.com;
```

20. Run the command **pdp m u a** to see all identities.
    - PDP is the policy decision point. This process acquires identities from identity sources and shares them with other gateways, known as identity sharing.



```
[Expert@GW:0]# pdp m u a

Session:  7e6da18f
Session UUID:  {14AD8EC0-ECC7-995F-09E8-A2EAA2FE761A}
Ip:  10.1.1.222
Users:
 t1_admin@americas-ses.com {cbbad187}
   LogUsername: t1_admin (t1_admin)
   Groups: All Users;ad_user_t1_admin
   Roles: allowed_streamers
   Client Type: AD Query
   Authentication Method: Trust
   Distinguished Name: CN=t1_admin,CN=Users,DC=americas-ses,DC=com
   Connect Time: Sun Nov  3 17:56:02 2024
   Next Reauthentication: Mon Nov  4 06:26:39 2024
   Next Connectivity Check: Mon Nov  4 06:26:39 2024
   Next Ldap Fetch: Sun Nov  3 21:17:41 2024

Packet Tagging Status:  Not Active
Published Gateways:  Local
**************************************************************************************
```

21. Run the command **pep sh u a** to see known identities to the PEP processes.
    - PEP is the policy enforcement point. This process receives identities shared from other gateways and redirects users to Captive Portal (more details in a later exercise).

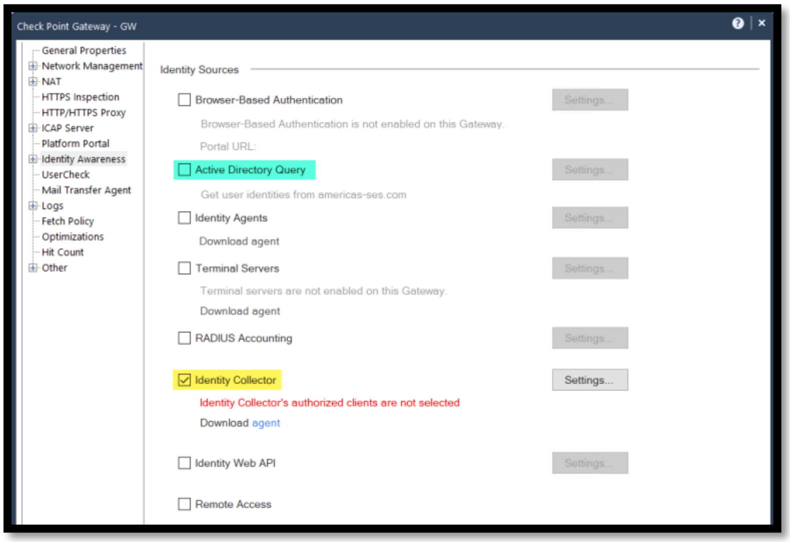


```
[Expert@GW:0]# pep show user a
Command: root->show->user->all
ID (PDP; UID)                       Username@Machine                   CID (IP, PacketID)            PT
============================================================================================================
127.0.0.1      :00000000; 7e6da18f  t1_admin@win-client                10.1.1.222                  , 00000000  -
127.0.0.1      :00000000; 0296d3e8  @server-22                         10.1.2.250                  , 00000000  -
```

# Exercise 2: Identity Collector

ADQuery uses WMI processes on the domain controller. There is performance degradation related to this design. To solve this problem among other issues, Check Point developed a new tool called Identity Collector.
Check Point Identity Collector is a dedicated client agent installed on Windows Servers in your network. Identity Collector collects information about identities and their associated IP addresses and sends it to the Check Point Security Gateway for identity enforcement.

1. Edit the GW object and **uncheck Active Directory Query** and enable the **Identity Collector**.



Check Point Gateway - GW

Identity Sources

□ Browser-Based Authentication — Settings...
Browser-Based Authentication is not enabled on this Gateway.
Portal URL:

□ Active Directory Query — Settings...
Get user identities from americas-ses.com

□ Identity Agents — Settings...
Download agent

□ Terminal Servers — Settings...
Terminal servers are not enabled on this Gateway.
Download agent

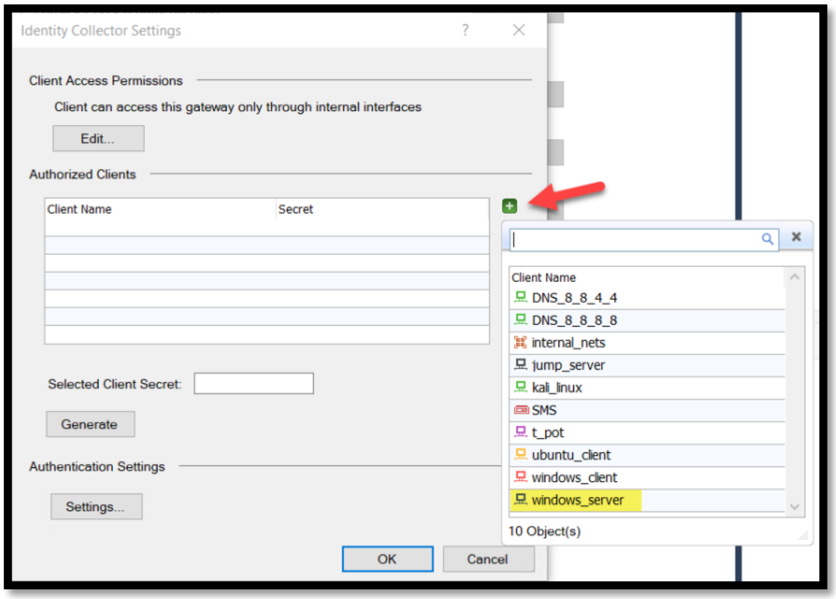
□ RADIUS Accounting — Settings...

☑ Identity Collector — Settings...
Identity Collector's authorized clients are not selected
Download agent

□ Identity Web API — Settings...

□ Remote Access

2. Click **Settings** and add the windows_server as an authorized client.



Identity Collector Settings

Client Access Permissions
Client can access this gateway only through internal interfaces
Edit...

Authorized Clients

| Client Name | Secret |
|---|---|

Selected Client Secret:
Generate

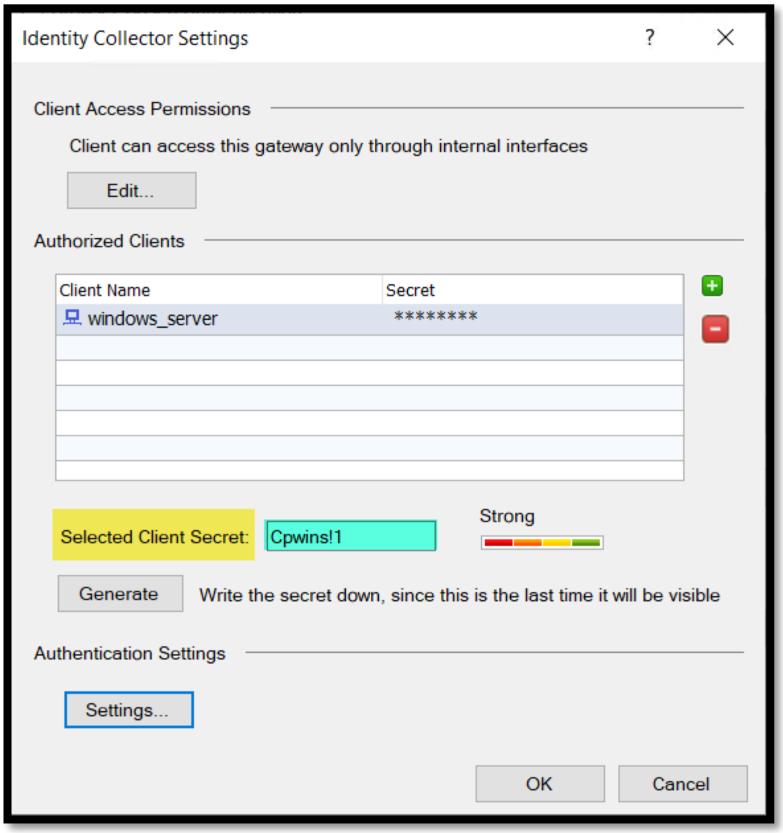
Authentication Settings
Settings...

OK Cancel

| Client Name |
|---|
| DNS_8_8_4_4 |
| DNS_8_8_8_8 |
| internal_nets |
| jump_server |
| kali_linux |
| SMS |
| t_pot |
| ubuntu_client |
| windows_client |
| windows_server |

10 Object(s)

3. Keep the generated client secret or type one manually. We will use this code later.



Identity Collector Settings

Client Access Permissions

Client can access this gateway only through internal interfaces

Edit...

Authorized Clients

| Client Name | Secret |
|---|---|
| windows_server | ******** |

Selected Client Secret: Cpwins!1

Strong

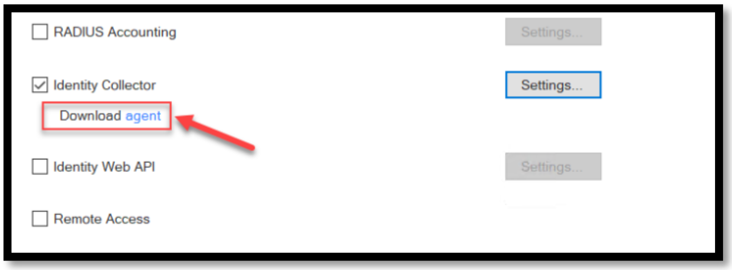
Generate   Write the secret down, since this is the last time it will be visible

Authentication Settings

Settings...

OK   Cancel

4. Click OK to return to the Identity Sources configurations. Click on the link to download the Identity Collector Agent. *The agents are also available inside the training project on GitHub*.
   - https://support.checkpoint.com/results/sk/sk134312



□ RADIUS Accounting   Settings...

☑ Identity Collector   Settings...

Download agent

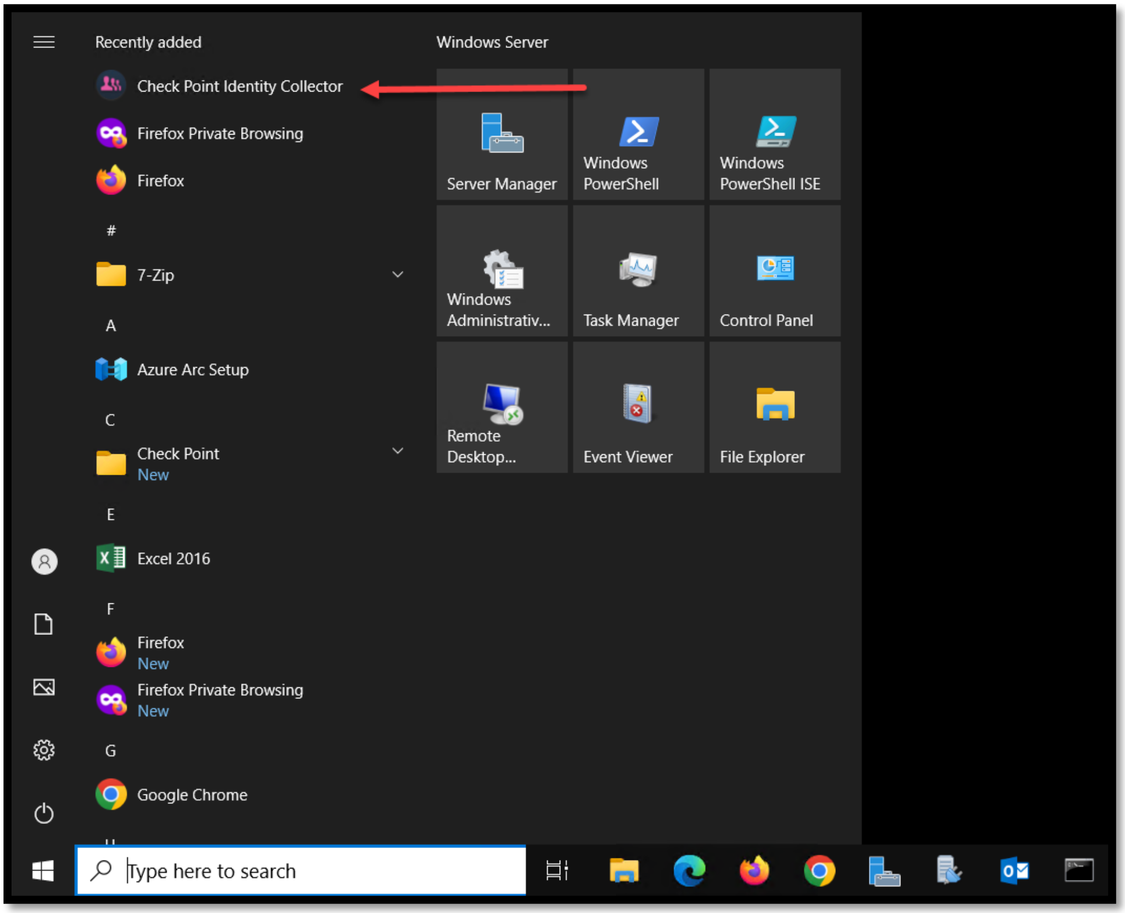
□ Identity Web API   Settings...

□ Remote Access

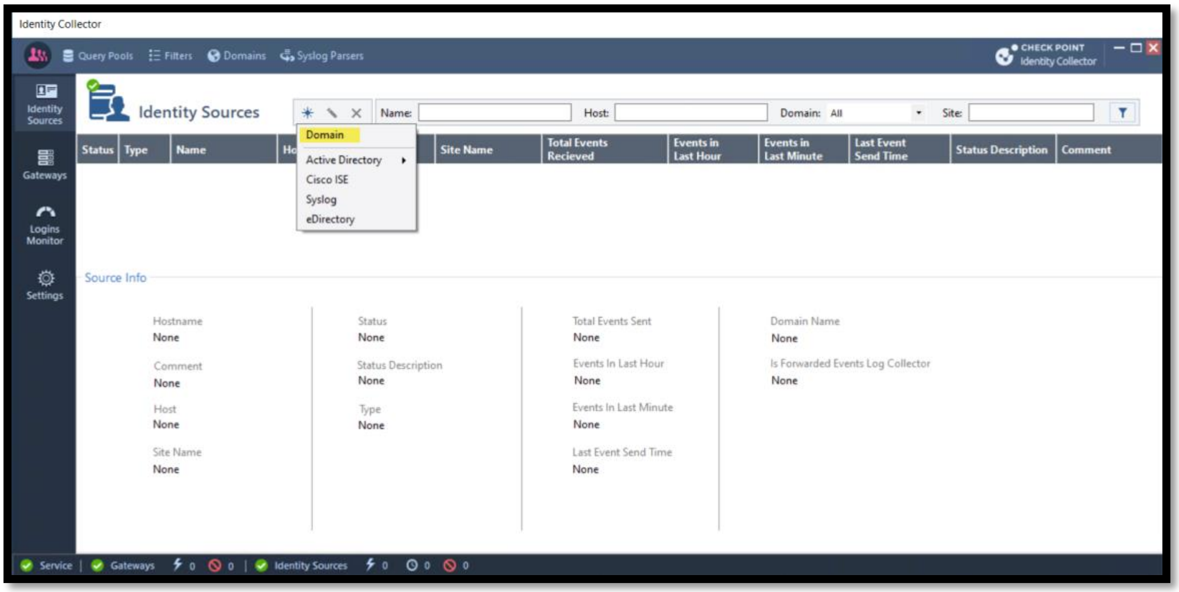
5. While the file is downloading, **Install the Access Policy**.

6. Copy the installation file to the Windows Server and install the agent.

7. Open the Identity Collector tool.



8. While in the default Identity Sources tab, add a new domain.



Hostname
None

Comment
None

Host
None

Site Name
None

Status
None

Status Description
None

Type
None

Total Events Sent
None

Events In Last Hour
None

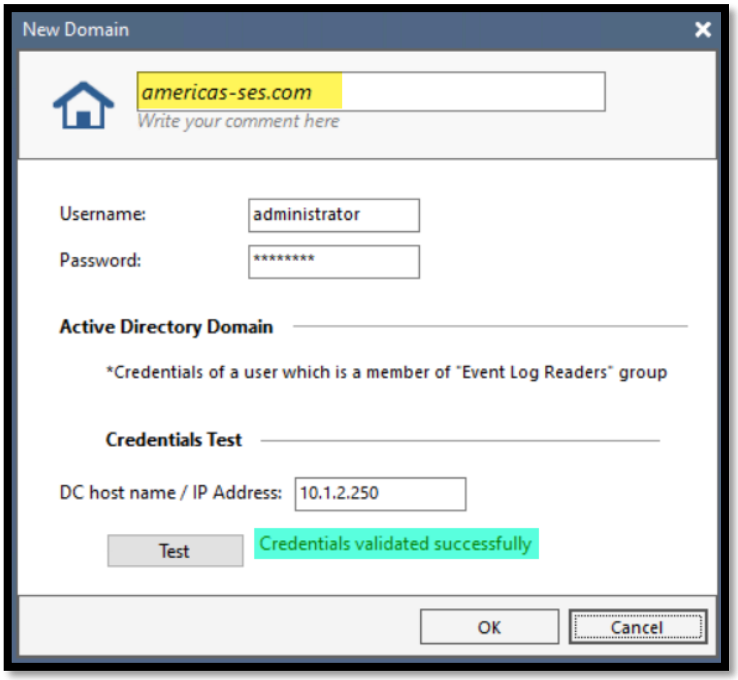
Events In Last Minute
None

Last Event Send Time
None

Domain Name
None

Is Forwarded Events Log Collector
None

9. Provide the Domain Controller details. Test the credentials and click OK.



americas-ses.com

Write your comment here

Username: administrator

Password: ********

Active Directory Domain

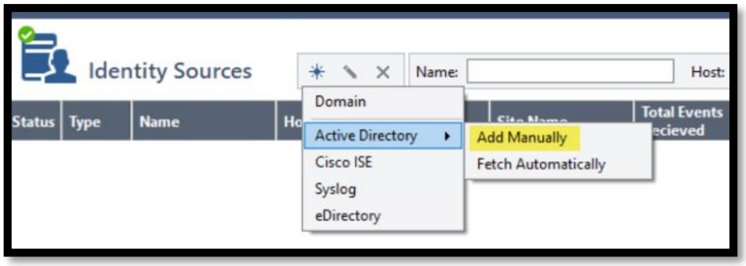
*Credentials of a user which is a member of "Event Log Readers" group

Credentials Test

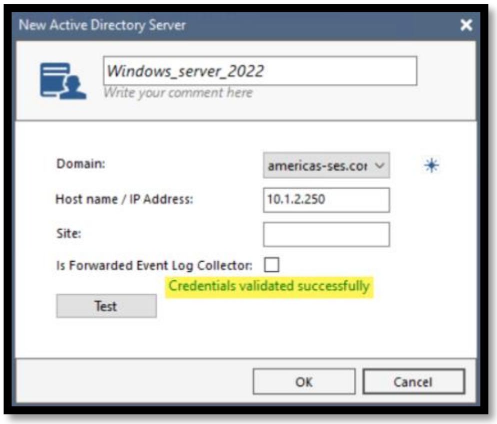
DC host name / IP Address: 10.1.2.250

Credentials validated successfully

10. Add a new Active Directory manually.



11. Provide the details and test the connection and click OK to exit the window.



Windows_server_2022

Write your comment here

Domain: americas-ses.cor

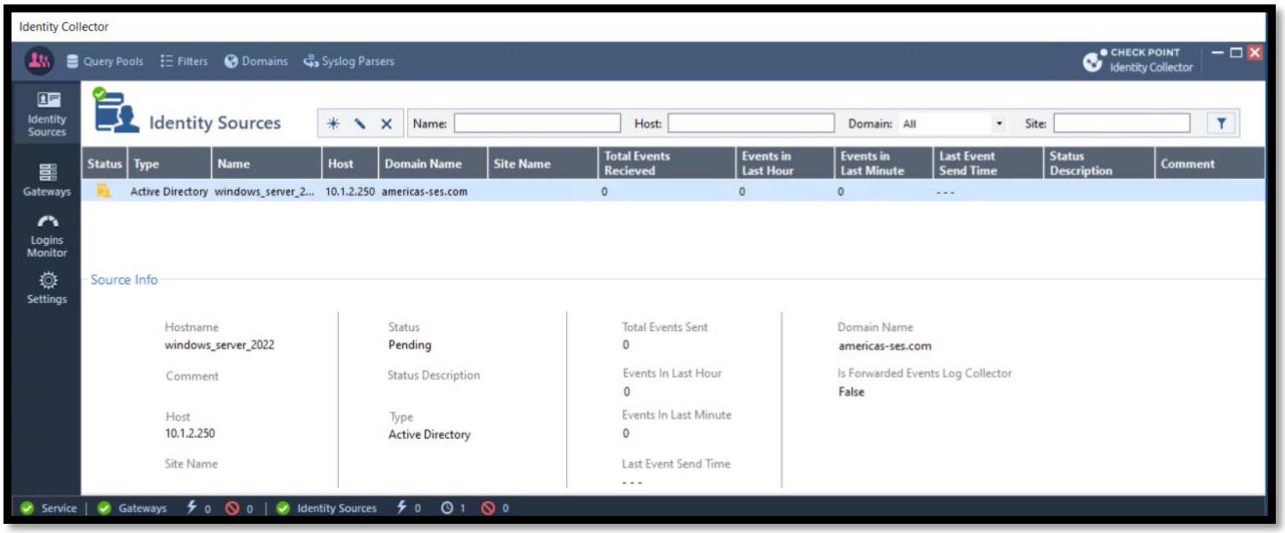
Host name / IP Address: 10.1.2.250

Site:

Is Forwarded Event Log Collector: □

Credentials validated successfully

12. By this stage, the identity collector is configured to collect logs from the domain controller of the domain Americas-ses.com



| Status | Type | Name | Host | Domain Name | Site Name | Total Events Recieved | Events in Last Hour | Events in Last Minute | Last Event Send Time | Status Description | Comment |
|---|---|---|---|---|---|---|---|---|---|---|---|
|  | Active Directory | windows_server_2... | 10.1.2.250 | americas-ses.com |  | 0 | 0 | 0 | - - - |  |  |

Source Info

Hostname
windows_server_2022

Comment

Host
10.1.2.250

Site Name

Status
Pending

Status Description

Type
Active Directory

Total Events Sent
0

Events In Last Hour
0

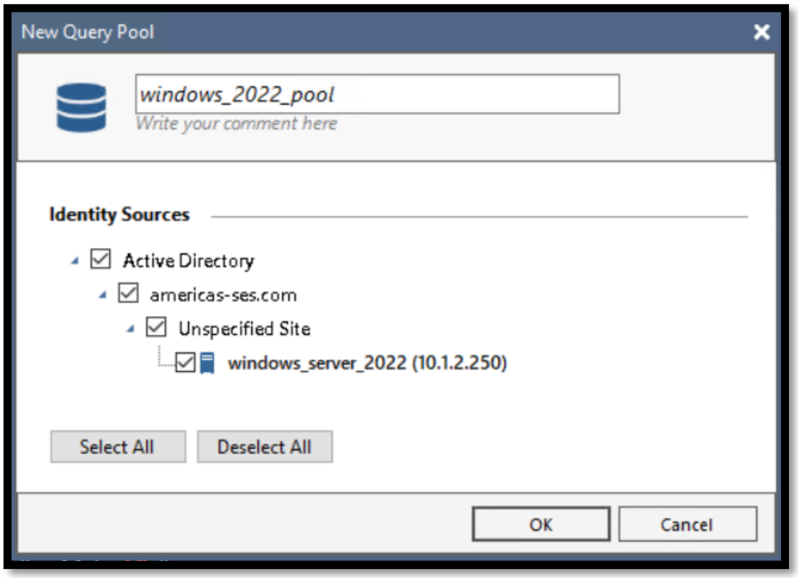
Events In Last Minute
0

Last Event Send Time
- - -

Domain Name
americas-ses.com

Is Forwarded Events Log Collector
False

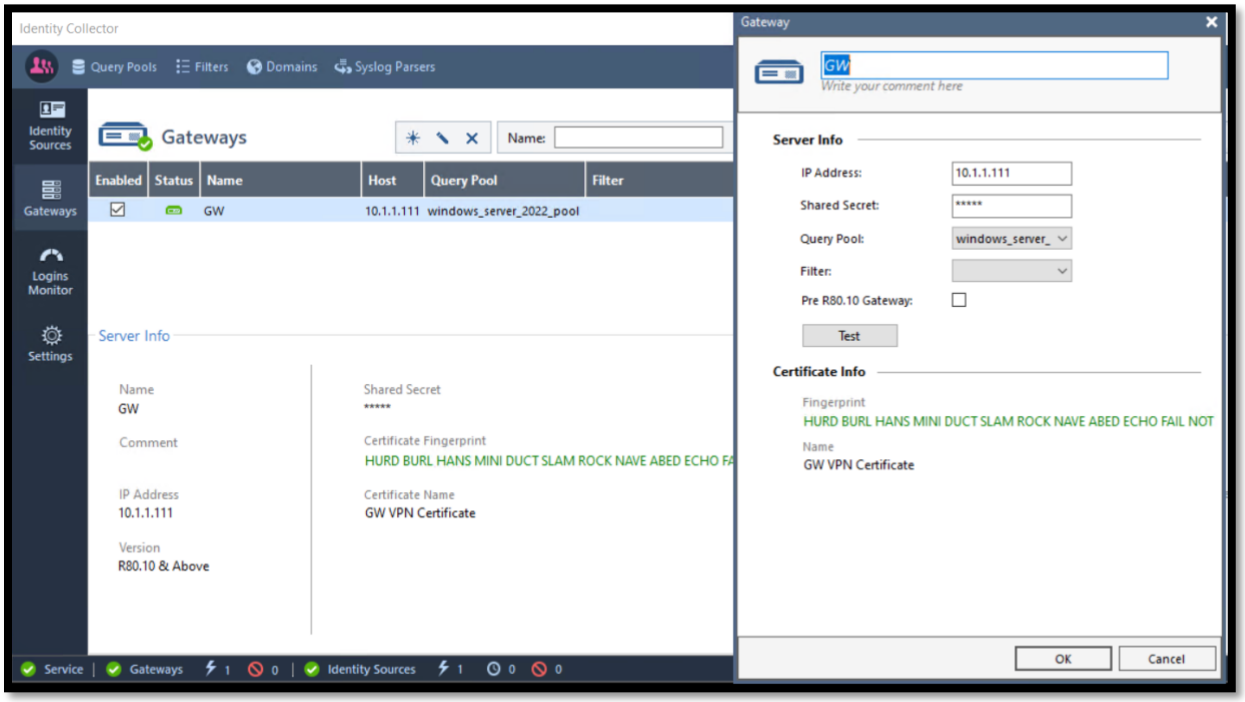
13. Click on Query Pools at the very top of the panel on the left to create a new query tool. This pool decided which events are forwarded to which GW.



*windows_2022_pool*
*Write your comment here*

- ☑ Active Directory
  - ☑ americas-ses.com
    - ☑ Unspecified Site
      - ☑ windows_server_2022 (10.1.2.250)

14. Move to the Gateway section, add a new Gateway configuration. Use the secret we configured on the GW object in SmartConsole earlier.



Identity Collector

Gateways

Name:

| Enabled | Status | Name | Host | Query Pool | Filter |
|---|---|---|---|---|---|
| ☑ | 🟩 | GW | 10.1.1.111 | windows_server_2022_pool | |

Server Info

Name
GW

Comment

IP Address
10.1.1.111

Version
R80.10 & Above

Shared Secret
*****

Certificate Fingerprint
HURD BURL HANS MINI DUCT SLAM ROCK NAVE ABED ECHO FA

Certificate Name
GW VPN Certificate

Gateway

GW
*Write your comment here*

Server Info

IP Address: 10.1.1.111
Shared Secret: *****
Query Pool: windows_server_
Filter:
Pre R80.10 Gateway: □

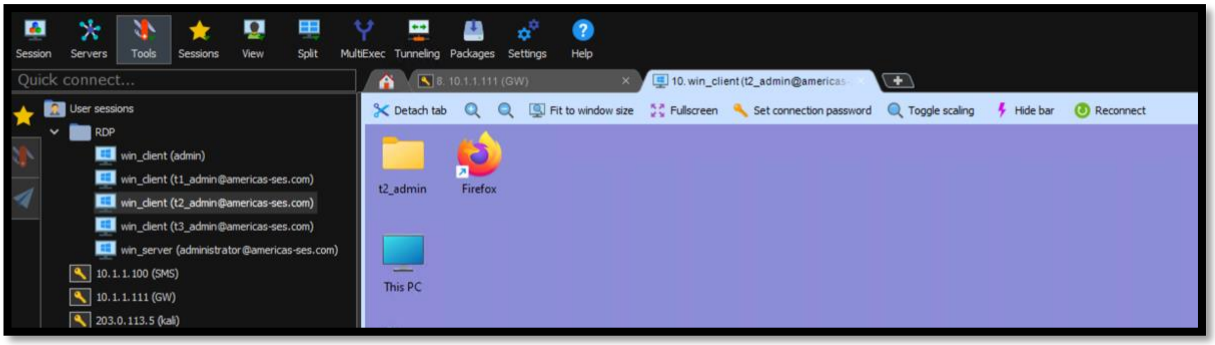
Certificate Info

Fingerprint
HURD BURL HANS MINI DUCT SLAM ROCK NAVE ABED ECHO FAIL NOT

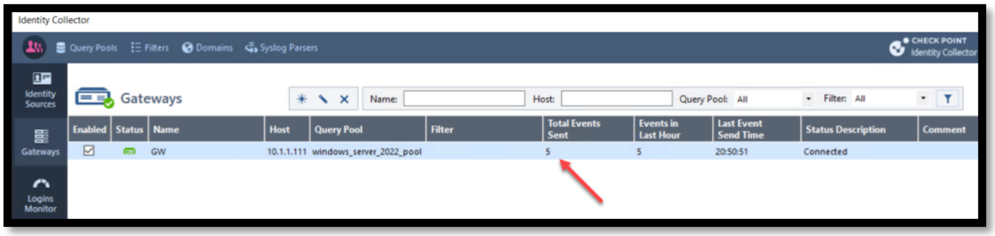
Name
GW VPN Certificate

- Notice that the self-signed certificate is presented. **Trust** it to complete the setup.
- We will not use filters, but we need to specify the query pool we created in the previous step.

15. Generate a login from the windows client machine. Login as t2_admin



16. Check the status of the Identity collector and notice that the GW has received some events



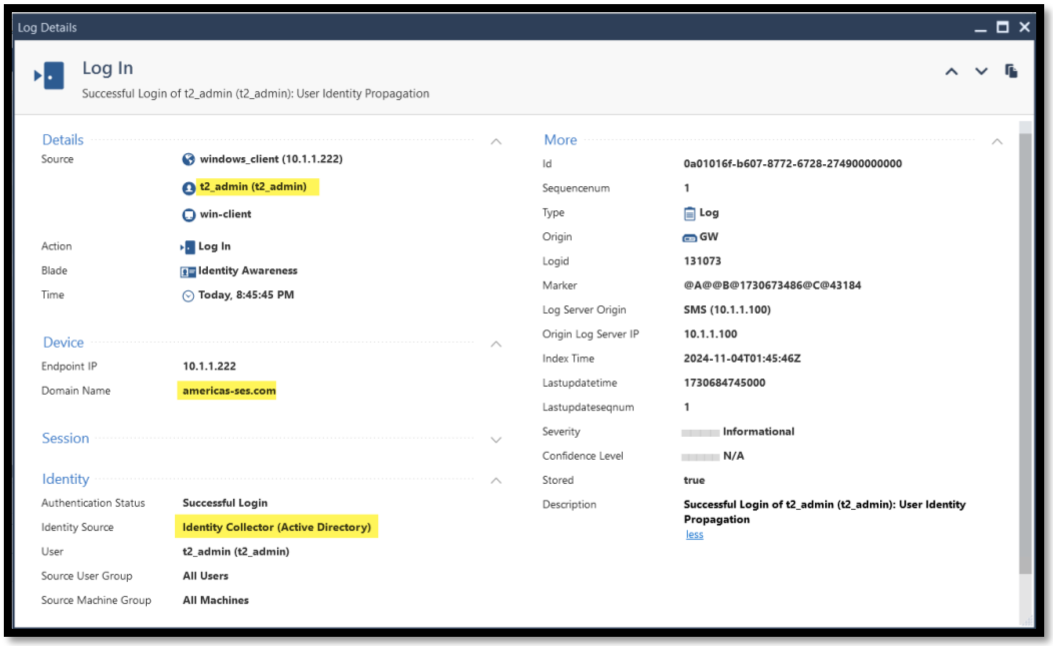
Identity Collector

Gateways

Name: Host: Query Pool: All Filter: All

| Enabled | Status | Name | Host | Query Pool | Filter | Total Events Sent | Events in Last Hour | Last Event Send Time | Status Description | Comment |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 🟩 | GW | 10.1.1.111 | windows_server_2022_pool | | 5 | 5 | 20:50:51 | Connected | |

17. Review the identity awareness logs and confirm the identity was acquired successfully.



Log Details

**Log In**

Successful Login of t2_admin (t2_admin): User Identity Propagation

**Details**

| | |
|---|---|
| Source | windows_client (10.1.1.222)<br>t2_admin (t2_admin)<br>win-client |
| Action | Log In |
| Blade | Identity Awareness |
| Time | Today, 8:45:45 PM |

**Device**

| | |
|---|---|
| Endpoint IP | 10.1.1.222 |
| Domain Name | americas-ses.com |

**Session**

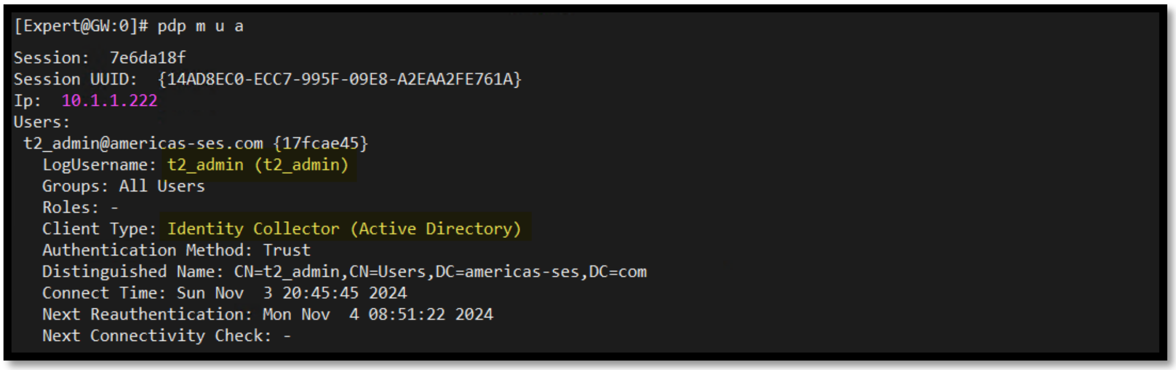
**Identity**

| | |
|---|---|
| Authentication Status | Successful Login |
| Identity Source | Identity Collector (Active Directory) |
| User | t2_admin (t2_admin) |
| Source User Group | All Users |
| Source Machine Group | All Machines |

**More**

| | |
|---|---|
| Id | 0a01016f-b607-8772-6728-274900000000 |
| Sequencenum | 1 |
| Type | Log |
| Origin | GW |
| Logid | 131073 |
| Marker | @A@@B@1730673486@C@43184 |
| Log Server Origin | SMS (10.1.1.100) |
| Origin Log Server IP | 10.1.1.100 |
| Index Time | 2024-11-04T01:45:46Z |
| Lastupdatetime | 1730684745000 |
| Lastupdateseqnum | 1 |
| Severity | Informational |
| Confidence Level | N/A |
| Stored | true |
| Description | Successful Login of t2_admin (t2_admin): User Identity Propagation<br>less |

18. Connect to the GW over SSH and Run the command **pdp m u a**.

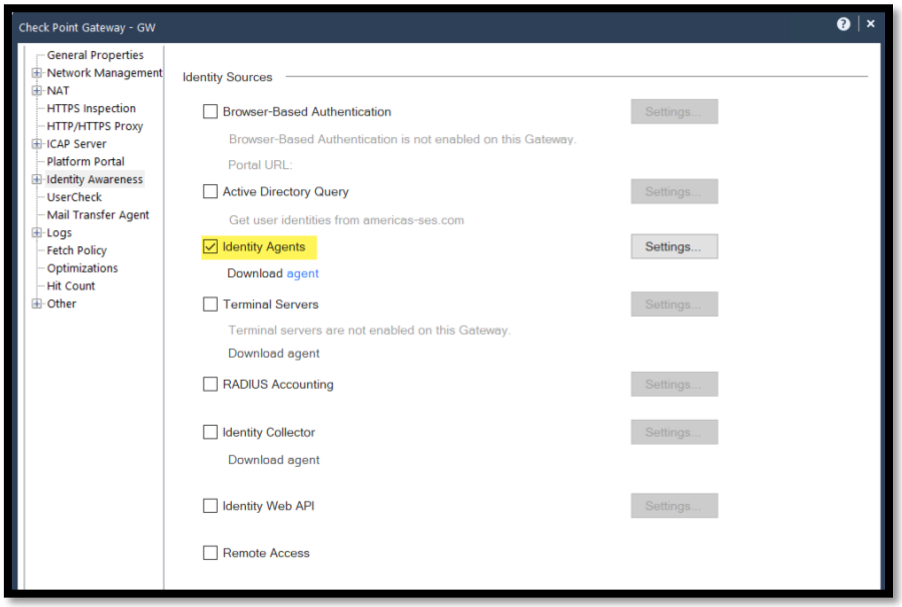


```
[Expert@GW:0]# pdp m u a

Session:  7e6da18f
Session UUID:  {14AD8EC0-ECC7-995F-09E8-A2EAA2FE761A}
Ip:  10.1.1.222
Users:
 t2_admin@americas-ses.com {17fcae45}
   LogUsername: t2_admin (t2_admin)
   Groups: All Users
   Roles: -
   Client Type: Identity Collector (Active Directory)
   Authentication Method: Trust
   Distinguished Name: CN=t2_admin,CN=Users,DC=americas-ses,DC=com
   Connect Time: Sun Nov  3 20:45:45 2024
   Next Reauthentication: Mon Nov  4 08:51:22 2024
   Next Connectivity Check: -
```

## Exercise 3: Identity Agents

There are scenarios where the user machine is not a part of the domain controller. In some cases, there are different reasons that prevents us from acquiring the identity via ADQuery or Identity Collector. In some cases, the ser might not exist on the domain controller but still needs to be authorized. We will use the Chek Point Identity Awareness Agent to acquire the identity and send it to the GW.

1. Edit the GW object and Enable the Identity Agent and disable the Identity Collector.



Identity Sources

□ Browser-Based Authentication
Browser-Based Authentication is not enabled on this Gateway.
Portal URL:

□ Active Directory Query
Get user identities from americas-ses.com

☑ Identity Agents
Download agent

□ Terminal Servers
Terminal servers are not enabled on this Gateway.
Download agent

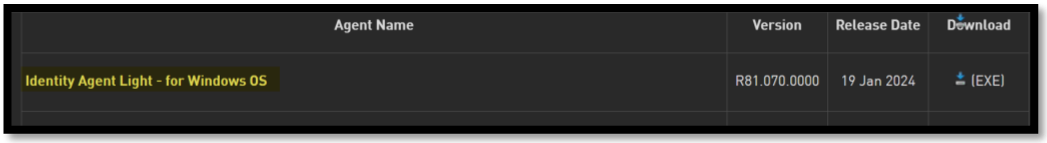
□ RADIUS Accounting

□ Identity Collector
Download agent

□ Identity Web API

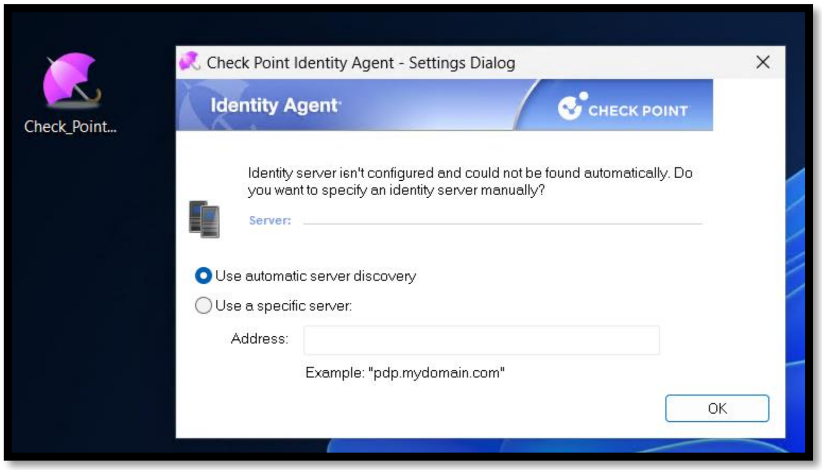
□ Remote Access

2. Click OK and install the Access Control policy.
3. Download the lightweight agent via the link. This is the same SK where we downloaded the Identity Collector. All other clients are also available for download.



| Agent Name | Version | Release Date | Download |
|---|---|---|---|
| Identity Agent Light - for Windows OS | R81.070.0000 | 19 Jan 2024 | (EXE) |

4. Log in to the windows client machine over RDP. The saved session on the Jump Server desktop is configured with the **local** account admin/Cpwins!1 which is not a domain user. Copy and Install the identity agent we just downloaded.



Identity server isn't configured and could not be found automatically. Do you want to specify an identity server manually?

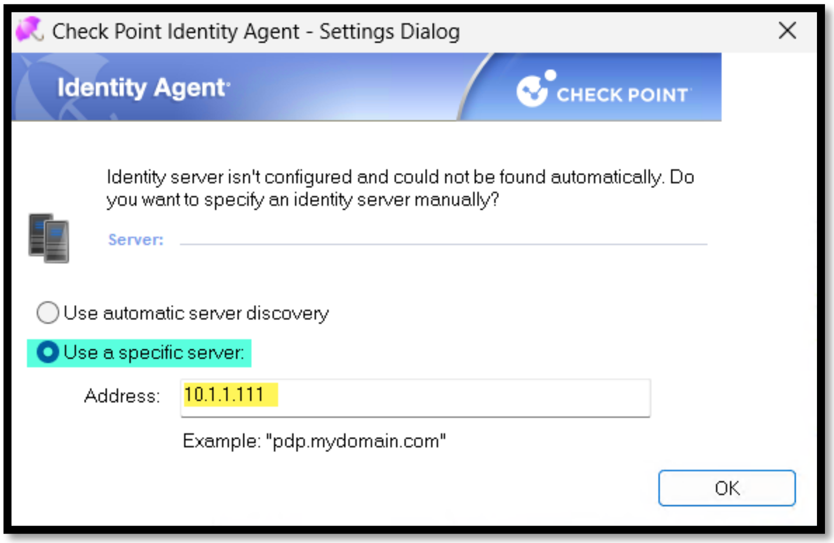
Server:

● Use automatic server discovery
○ Use a specific server:

Address:

Example: "pdp.mydomain.com"

5. Select Use a specific server and provide the GW IP address and click OK.



Check Point Identity Agent - Settings Dialog

Identity server isn't configured and could not be found automatically. Do you want to specify an identity server manually?

Server:

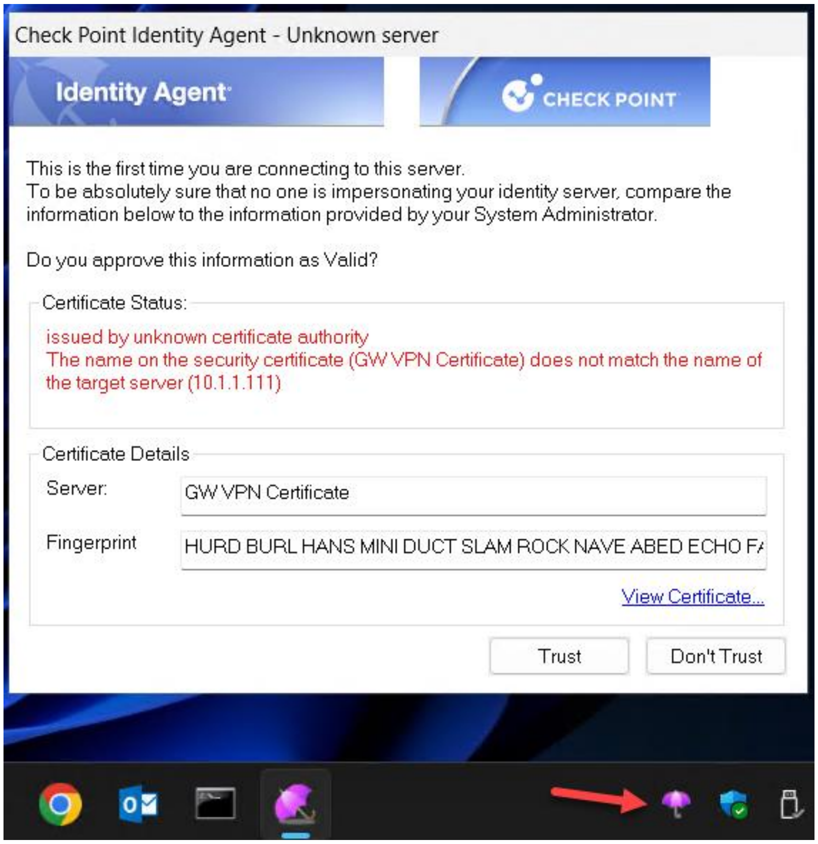
○ Use automatic server discovery

● Use a specific server:

Address: 10.1.1.111

Example: "pdp.mydomain.com"

6. Like connecting via the identity collector, the Agent is presented with the default VPN certificate. Trust it and continue.



Check Point Identity Agent - Unknown server

This is the first time you are connecting to this server.
To be absolutely sure that no one is impersonating your identity server, compare the information below to the information provided by your System Administrator.

Do you approve this information as Valid?

Certificate Status:

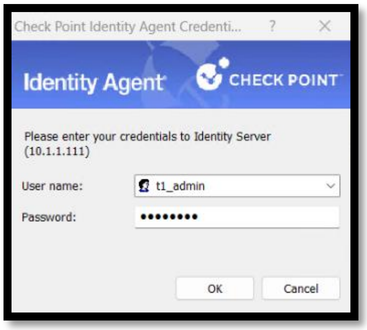
issued by unknown certificate authority
The name on the security certificate (GW VPN Certificate) does not match the name of the target server (10.1.1.111)

Certificate Details

Server: GW VPN Certificate

Fingerprint HURD BURL HANS MINI DUCT SLAM ROCK NAVE ABED ECHO F/

7. You will be forwarded to provide your identity. Login as t1_admin/Cpwins!1. This is the user we added in the allowed_streamers access role to grant access to YouTube.



Check Point Identity Agent Credenti...

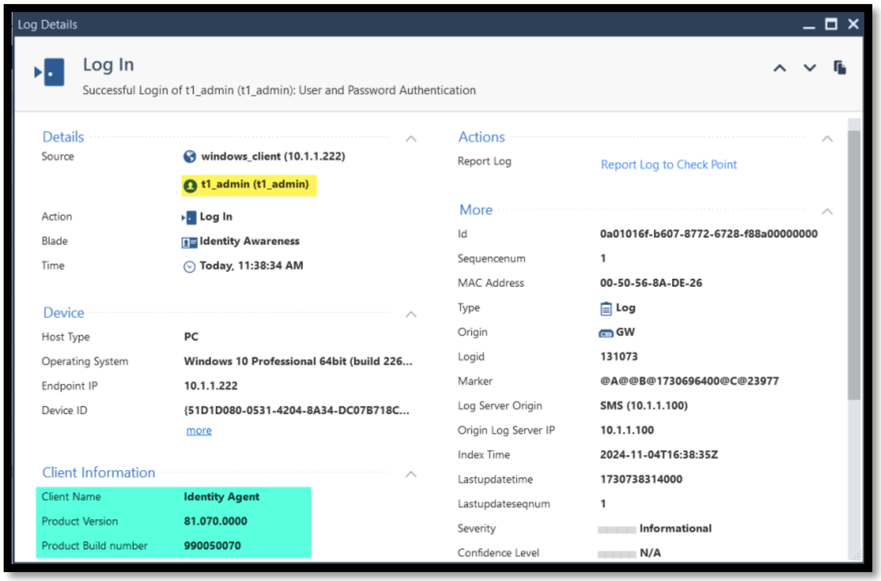
Identity Agent

Please enter your credentials to Identity Server (10.1.1.111)

User name: t1_admin

Password: ••••••••

8. Review the identity Awareness logs and notice that the identity was acquired successfully,



Log Details

Log In

Successful Login of t1_admin (t1_admin): User and Password Authentication

Details

Source: windows_client (10.1.1.222)
t1_admin (t1_admin)

Action: Log In

Blade: Identity Awareness

Time: Today, 11:38:34 AM

Device

Host Type: PC

Operating System: Windows 10 Professional 64bit (build 226...

Endpoint IP: 10.1.1.222

Device ID: {51D1D080-0531-4204-8A34-DC07B718C...
more

Client Information

Client Name: Identity Agent

Product Version: 81.070.0000

Product Build number: 990050070

Actions

Report Log: Report Log to Check Point

More

Id: 0a01016f-b607-8772-6728-f88a00000000

Sequencenum: 1

MAC Address: 00-50-56-8A-DE-26

Type: Log

Origin: GW

Logid: 131073

Marker: @A@@B@1730696400@C@23977

Log Server Origin: SMS (10.1.1.100)

Origin Log Server IP: 10.1.1.100

Index Time: 2024-11-04T16:38:35Z

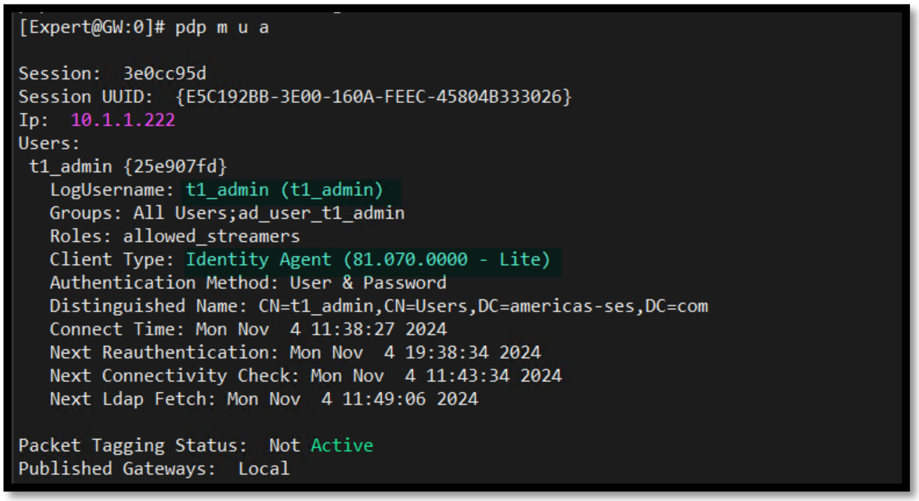
Lastupdatetime: 1730738314000

Lastupdateseqnum: 1

Severity: Informational

Confidence Level: N/A

9. Use the command **pdp m u a** to confirm that the user identity is known to PDP.



```
[Expert@GW:0]# pdp m u a

Session:  3e0cc95d
Session UUID:  {E5C192BB-3E00-160A-FEEC-45804B333026}
Ip:  10.1.1.222
Users:
 t1_admin {25e907fd}
   LogUsername: t1_admin (t1_admin)
   Groups: All Users;ad_user_t1_admin
   Roles: allowed_streamers
   Client Type: Identity Agent (81.070.0000 - Lite)
   Authentication Method: User & Password
   Distinguished Name: CN=t1_admin,CN=Users,DC=americas-ses,DC=com
   Connect Time: Mon Nov  4 11:38:27 2024
   Next Reauthentication: Mon Nov  4 19:38:34 2024
   Next Connectivity Check: Mon Nov  4 11:43:34 2024
   Next Ldap Fetch: Mon Nov  4 11:49:06 2024

Packet Tagging Status:  Not Active
Published Gateways:  Local
```

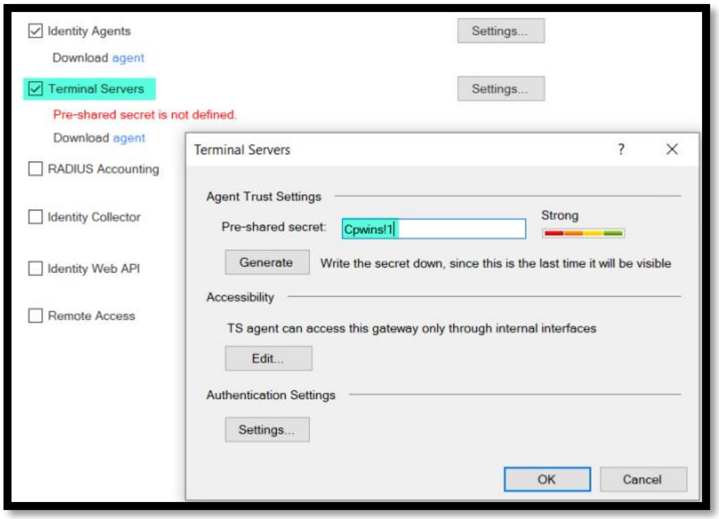
10. Try to reach YouTube and review the logs to confirm the traffic was allowed by the correct rule.

## Exercise 4: Terminal Servers Agent (MuH)

In the previous exercise, we used the Check Point identity agent to grant a user access. This will handle the authentication single user. There are different deployment scenarios where multiple users are using the same machine such as in terminal servers.

In this exercise, we will install the MuH agent on the windows server to handle multiple identities simultaneously.

1. Edit the GW object, Enable Terminal Servers. And click Settings to configure the Pre-shared secret.

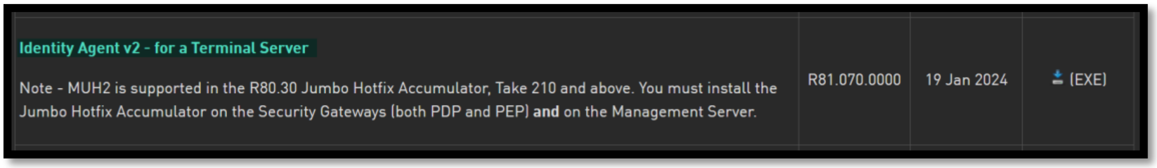


☑ Identity Agents — Settings...
Download agent
☑ Terminal Servers — Settings...
Pre-shared secret is not defined.
Download agent
☐ RADIUS Accounting
☐ Identity Collector
☐ Identity Web API
☐ Remote Access

Terminal Servers ? ✕

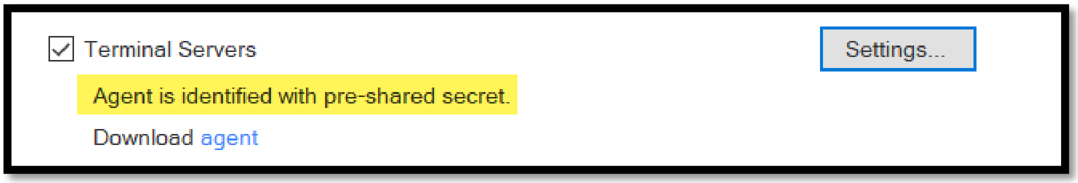
Agent Trust Settings
Pre-shared secret: Cpwins!1 — Strong
Generate — Write the secret down, since this is the last time it will be visible
Accessibility
TS agent can access this gateway only through internal interfaces
Edit...
Authentication Settings
Settings...
OK — Cancel

2. Download the Identity Agent v2 for terminal servers. Use the same SK we used to download the previous clients.



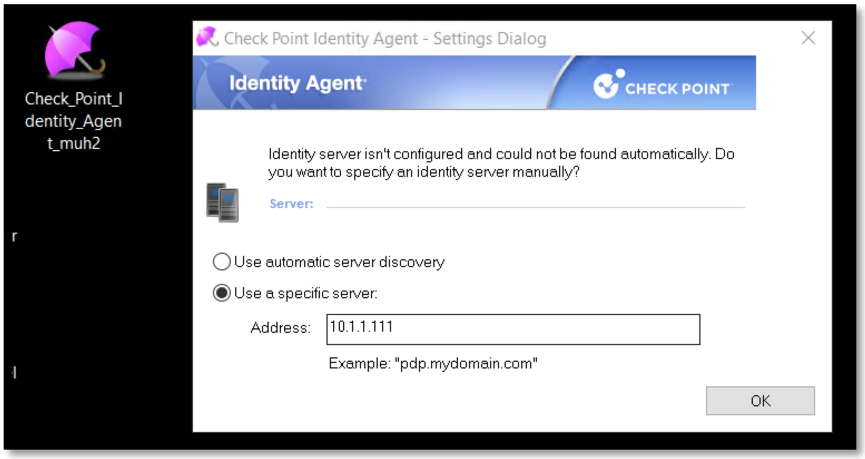
| | | | |
|---|---|---|---|
| **Identity Agent v2 - for a Terminal Server**<br>Note - MUH2 is supported in the R80.30 Jumbo Hotfix Accumulator, Take 210 and above. You must install the Jumbo Hotfix Accumulator on the Security Gateways (both PDP and PEP) **and** on the Management Server. | R81.070.0000 | 19 Jan 2024 | (EXE) |

3. Confirm the secret is confirmed and install the access policy.



☑ Terminal Servers — Settings...
Agent is identified with pre-shared secret.
Download agent

4. Copy the agent to the domain controller and install it. Configure it to connect to the GW over 10.1.1.111.



Check_Point_Identity_Agent_muh2
Check Point Identity Agent - Settings Dialog
Identity Agent
CHECK POINT

Identity server isn't configured and could not be found automatically. Do you want to specify an identity server manually?

Server:

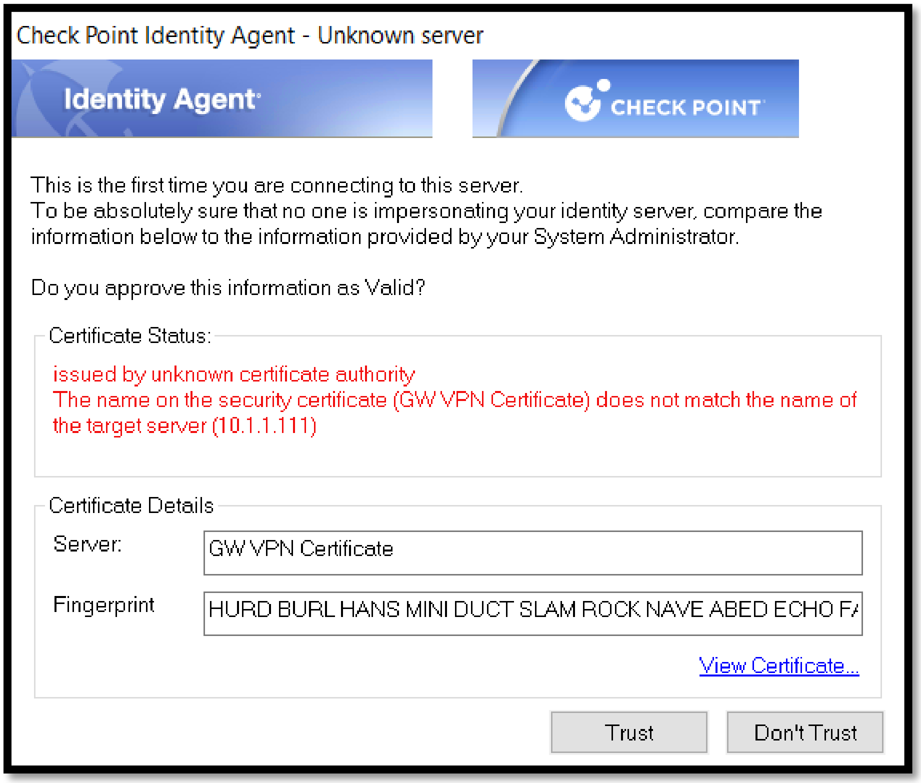
○ Use automatic server discovery

● Use a specific server:

Address: 10.1.1.111

Example: "pdp.mydomain.com"

5. Try to connect this agent and trust the self-signed certificate.



Check Point Identity Agent - Unknown server

This is the first time you are connecting to this server.
To be absolutely sure that no one is impersonating your identity server, compare the information below to the information provided by your System Administrator.

Do you approve this information as Valid?

Certificate Status:

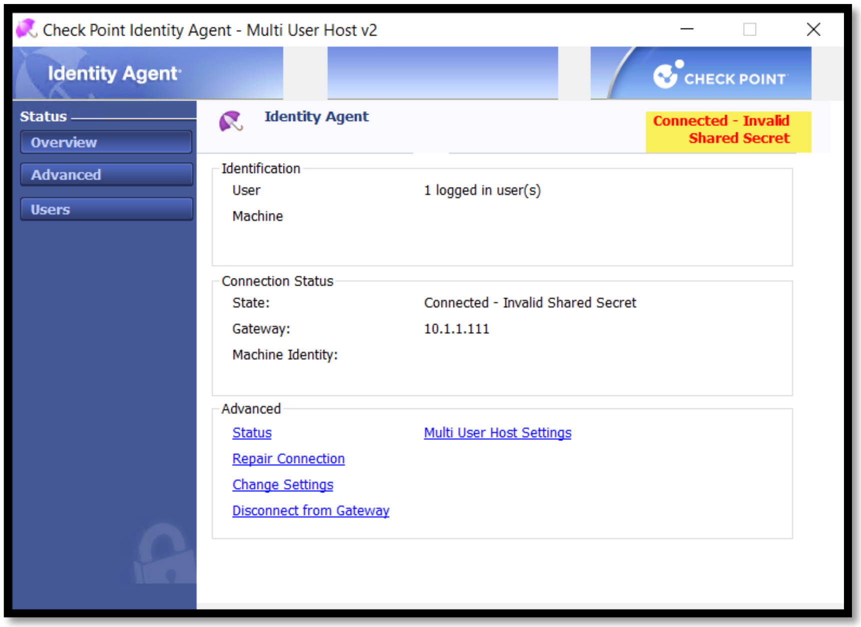
issued by unknown certificate authority
The name on the security certificate (GW VPN Certificate) does not match the name of the target server (10.1.1.111)

Certificate Details

Server: GW VPN Certificate

Fingerprint: HURD BURL HANS MINI DUCT SLAM ROCK NAVE ABED ECHO F/

6. Notice that the connection will fail since we have not configured the Shared Secret in the agent yet.



Check Point Identity Agent - Multi User Host v2

**Identity Agent** — **Connected - Invalid Shared Secret**

Identification

| | |
|---|---|
| User | 1 logged in user(s) |
| Machine | |

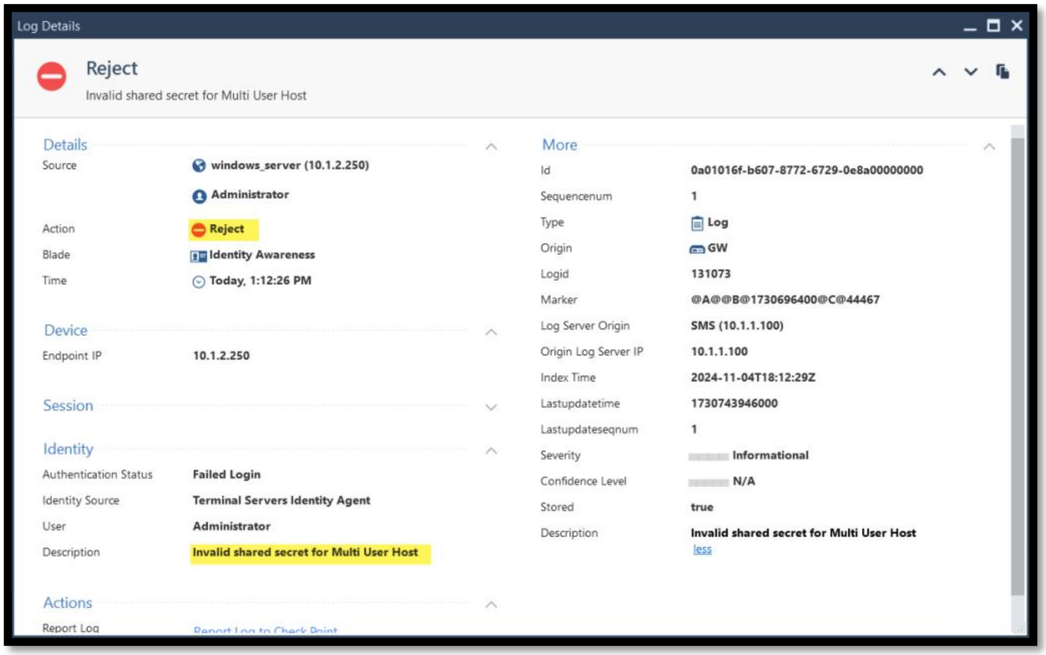
Connection Status

| | |
|---|---|
| State: | Connected - Invalid Shared Secret |
| Gateway: | 10.1.1.111 |
| Machine Identity: | |

Advanced

| | |
|---|---|
| Status | Multi User Host Settings |
| Repair Connection | |
| Change Settings | |
| Disconnect from Gateway | |

7. Review the Identity awareness logs and confirm you can see the related log.



Log Details

**Reject**
Invalid shared secret for Multi User Host

Details

| | |
|---|---|
| Source | windows_server (10.1.2.250)<br>Administrator |
| Action | Reject |
| Blade | Identity Awareness |
| Time | Today, 1:12:26 PM |

Device

| | |
|---|---|
| Endpoint IP | 10.1.2.250 |

Session

Identity

| | |
|---|---|
| Authentication Status | Failed Login |
| Identity Source | Terminal Servers Identity Agent |
| User | Administrator |
| Description | Invalid shared secret for Multi User Host |

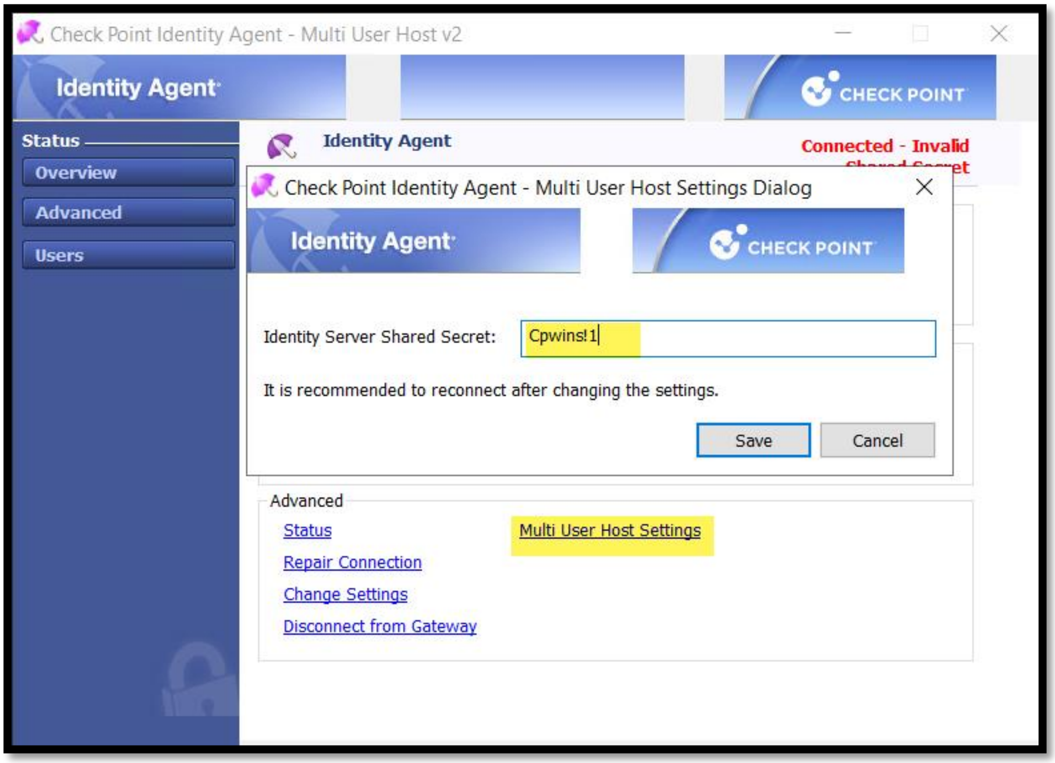
Actions

| | |
|---|---|
| Report Log | Report Log to Check Point |

More

| | |
|---|---|
| Id | 0a01016f-b607-8772-6729-0e8a00000000 |
| Sequencenum | 1 |
| Type | Log |
| Origin | GW |
| Logid | 131073 |
| Marker | @A@@B@1730696400@C@44467 |
| Log Server Origin | SMS (10.1.1.100) |
| Origin Log Server IP | 10.1.1.100 |
| Index Time | 2024-11-04T18:12:29Z |
| Lastupdatetime | 1730743946000 |
| Lastupdateseqnum | 1 |
| Severity | Informational |
| Confidence Level | N/A |
| Stored | true |
| Description | Invalid shared secret for Multi User Host<br>less |

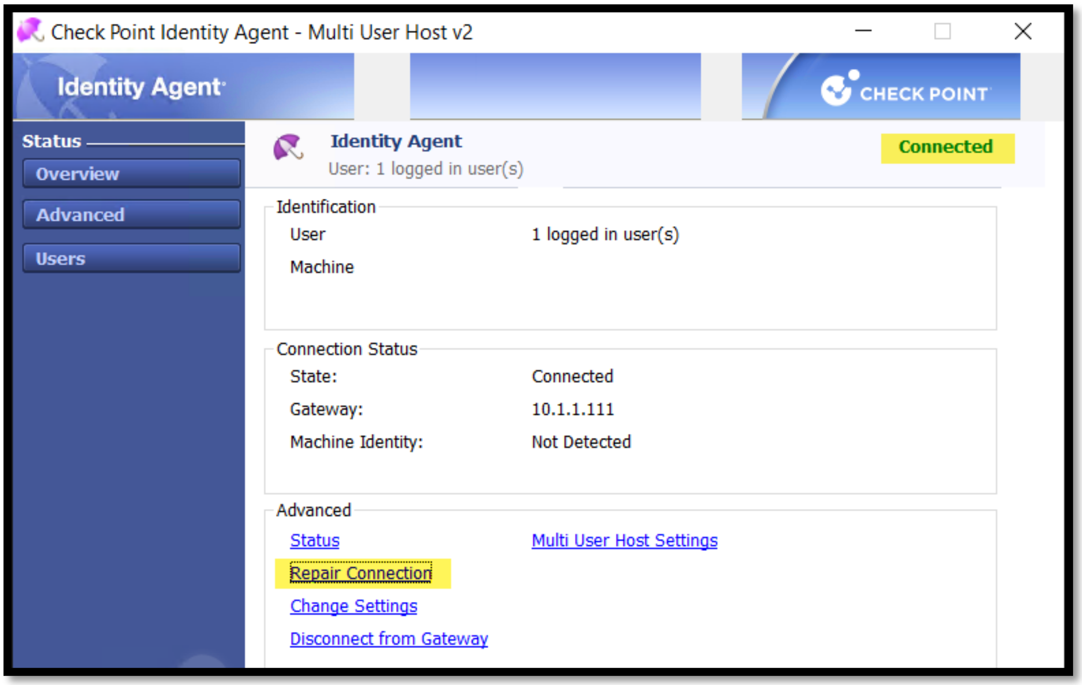
8. To enter the Shared Secret, click **Multi User Host Settings** and provide the secret we configured earlier and save the settings.



Identity Server Shared Secret: Cpwins!1

It is recommended to reconnect after changing the settings.

9. Try to connect again by repairing the connection and confirm the agent is now connected.



User: 1 logged in user(s)

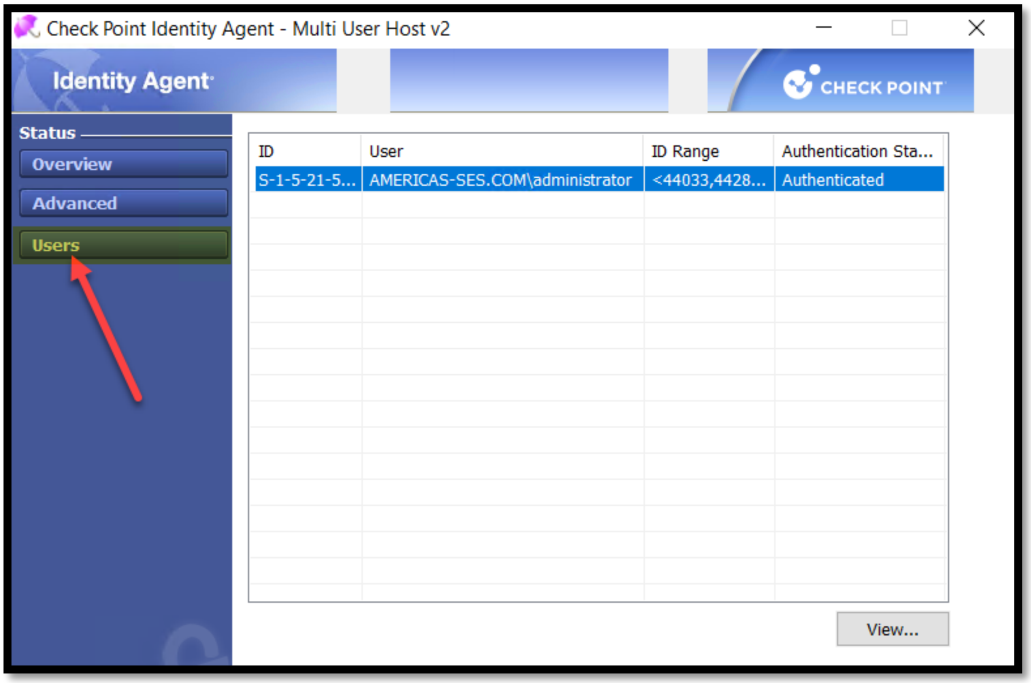
Identification

User 1 logged in user(s)
Machine

Connection Status

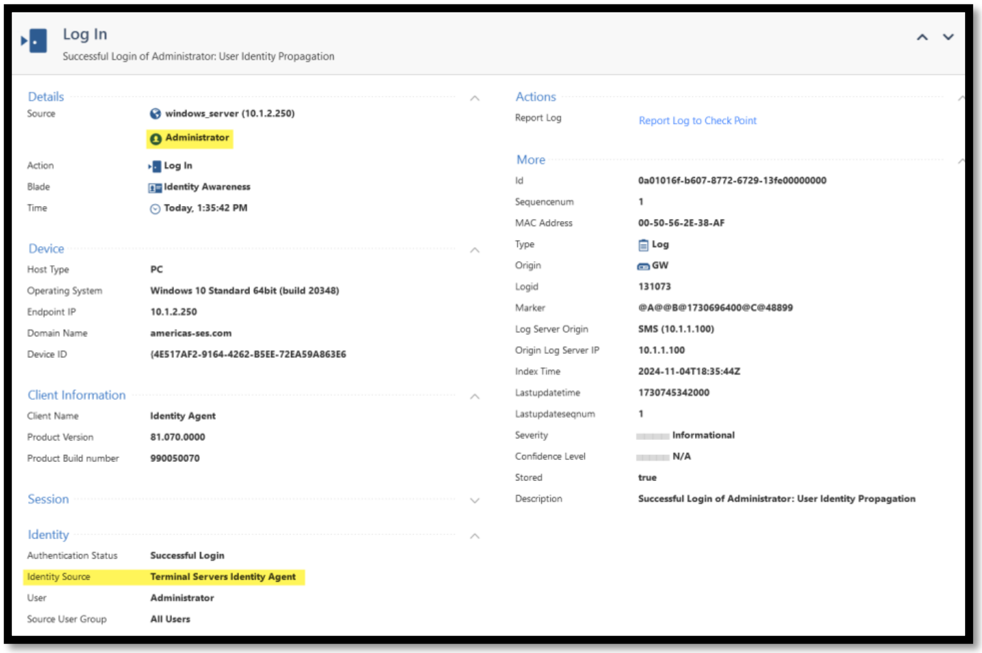
State: Connected
Gateway: 10.1.1.111
Machine Identity: Not Detected

10. Under the users list in the agent, confirm you can see the current user in the list as an authenticated user



| ID | User | ID Range | Authentication Sta... |
|---|---|---|---|
| S-1-5-21-5... | AMERICAS-SES.COM\administrator | <44033,4428... | Authenticated |

11. Review the logs and confirm the Administrator user was authenticated successfully.



**Log In**

Successful Login of Administrator: User Identity Propagation

**Details**

| | |
|---|---|
| Source | windows_server (10.1.2.250)<br>Administrator |
| Action | Log In |
| Blade | Identity Awareness |
| Time | Today, 1:35:42 PM |

**Device**

| | |
|---|---|
| Host Type | PC |
| Operating System | Windows 10 Standard 64bit (build 20348) |
| Endpoint IP | 10.1.2.250 |
| Domain Name | americas-ses.com |
| Device ID | {4E517AF2-9164-4262-B5EE-72EA59A863E6 |

**Client Information**

| | |
|---|---|
| Client Name | Identity Agent |
| Product Version | 81.070.0000 |
| Product Build number | 990050070 |

**Session**

**Identity**

| | |
|---|---|
| Authentication Status | Successful Login |
| Identity Source | Terminal Servers Identity Agent |
| User | Administrator |
| Source User Group | All Users |

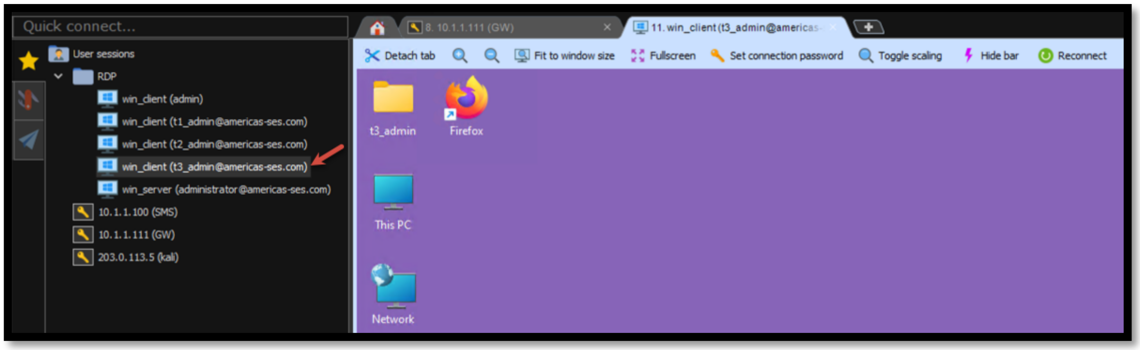
**Actions**

| | |
|---|---|
| Report Log | Report Log to Check Point |

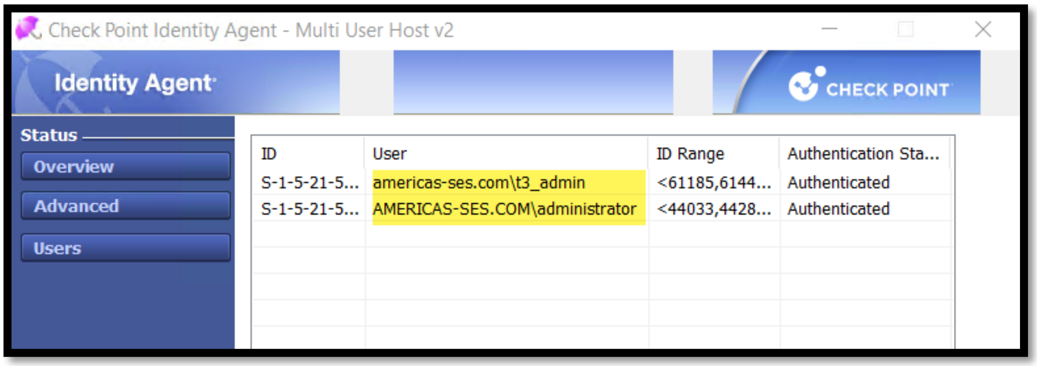
**More**

| | |
|---|---|
| Id | 0a01016f-b607-8772-6729-13fe00000000 |
| Sequencenum | 1 |
| MAC Address | 00-50-56-2E-38-AF |
| Type | Log |
| Origin | GW |
| Logid | 131073 |
| Marker | @A@@B@1730696400@C@48899 |
| Log Server Origin | SMS (10.1.1.100) |
| Origin Log Server IP | 10.1.1.100 |
| Index Time | 2024-11-04T18:35:44Z |
| Lastupdatetime | 1730745342000 |
| Lastupdateseqnum | 1 |
| Severity | Informational |
| Confidence Level | N/A |
| Stored | true |
| Description | Successful Login of Administrator: User Identity Propagation |

12. Return to the training environment and try to login with t3_admin/Cpwins!1 credentials.

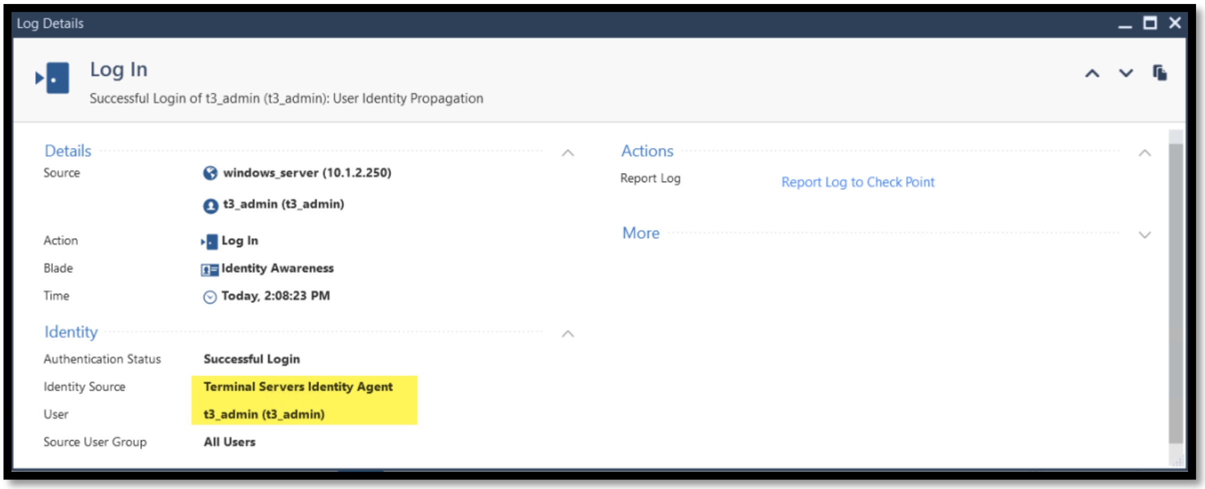


13. Return to the previous RDP connection and confirm that the new user is also identified



| ID | User | ID Range | Authentication Sta... |
|---|---|---|---|
| S-1-5-21-5... | americas-ses.com\t3_admin | <61185,6144... | Authenticated |
| S-1-5-21-5... | AMERICAS-SES.COM\administrator | <44033,4428... | Authenticated |

14. Review the logs and confirm the user is knows to the GW.

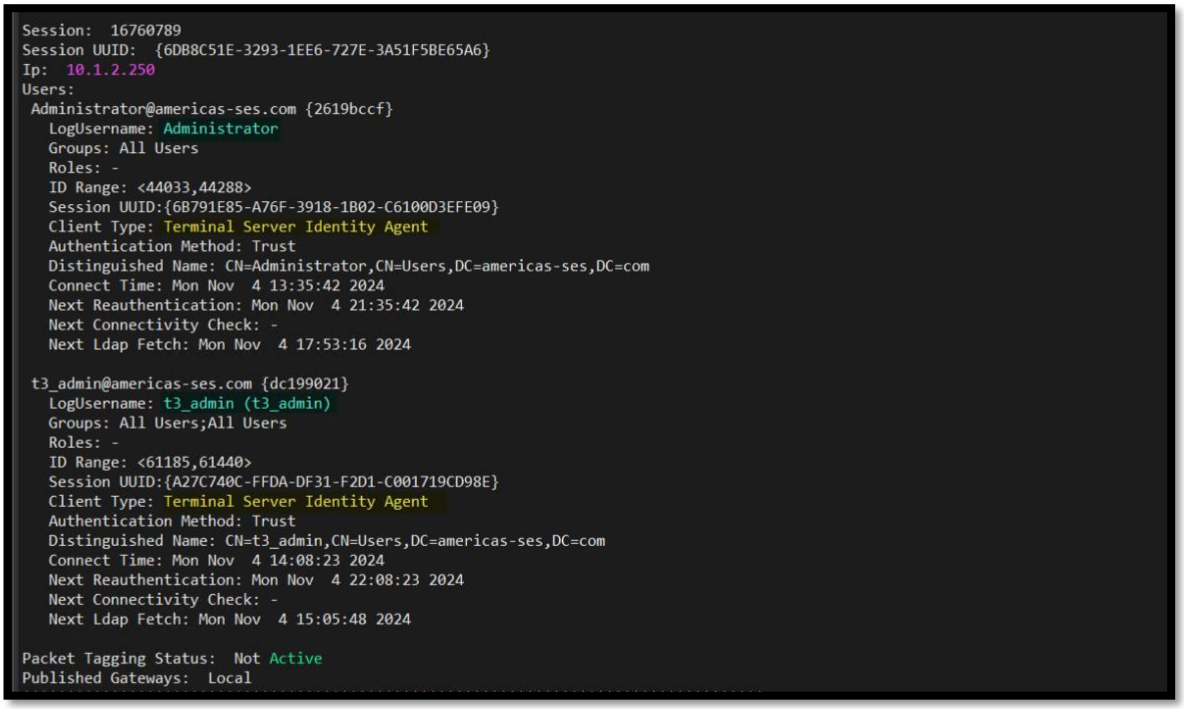


Log In

Successful Login of t3_admin (t3_admin): User Identity Propagation

| | |
|---|---|
| Source | windows_server (10.1.2.250)<br>t3_admin (t3_admin) |
| Action | Log In |
| Blade | Identity Awareness |
| Time | Today, 2:08:23 PM |
| Authentication Status | Successful Login |
| Identity Source | Terminal Servers Identity Agent |
| User | t3_admin (t3_admin) |
| Source User Group | All Users |
| Report Log | Report Log to Check Point |

15. Finally, use the command **pdp m u a** to confirm that all users are associated to the same host.



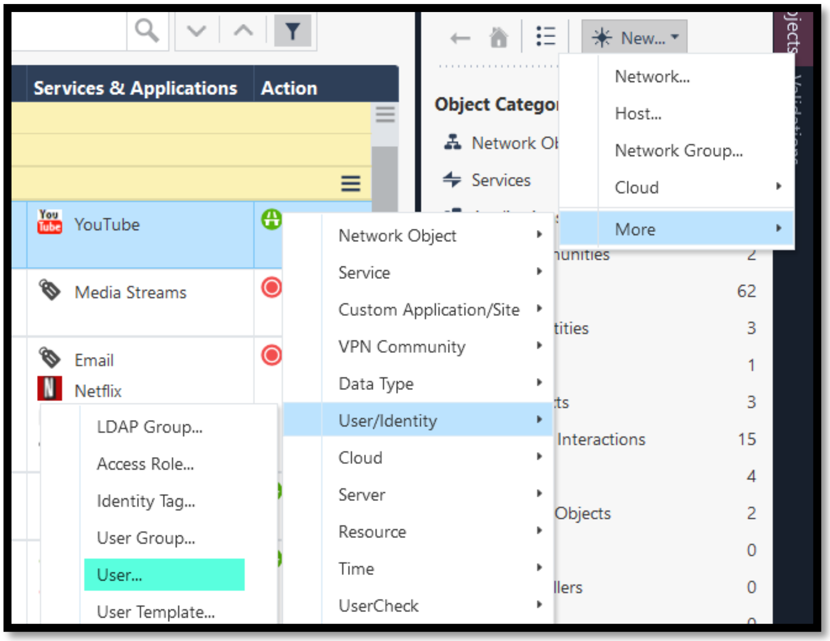
```
Session:  16760789
Session UUID:  {6DB8C51E-3293-1EE6-727E-3A51F5BE65A6}
Ip:  10.1.2.250
Users:
 Administrator@americas-ses.com {2619bccf}
   LogUsername: Administrator
   Groups: All Users
   Roles: -
   ID Range: <44033,44288>
   Session UUID:{6B791E85-A76F-3918-1B02-C6100D3EFE09}
   Client Type: Terminal Server Identity Agent
   Authentication Method: Trust
   Distinguished Name: CN=Administrator,CN=Users,DC=americas-ses,DC=com
   Connect Time: Mon Nov  4 13:35:42 2024
   Next Reauthentication: Mon Nov  4 21:35:42 2024
   Next Connectivity Check: -
   Next Ldap Fetch: Mon Nov  4 17:53:16 2024

 t3_admin@americas-ses.com {dc199021}
   LogUsername: t3_admin (t3_admin)
   Groups: All Users;All Users
   Roles: -
   ID Range: <61185,61440>
   Session UUID:{A27C740C-FFDA-DF31-F2D1-C001719CD98E}
   Client Type: Terminal Server Identity Agent
   Authentication Method: Trust
   Distinguished Name: CN=t3_admin,CN=Users,DC=americas-ses,DC=com
   Connect Time: Mon Nov  4 14:08:23 2024
   Next Reauthentication: Mon Nov  4 22:08:23 2024
   Next Connectivity Check: -
   Next Ldap Fetch: Mon Nov  4 15:05:48 2024

Packet Tagging Status:  Not Active
Published Gateways:  Local
```

## Exercise 5: Captive Portal

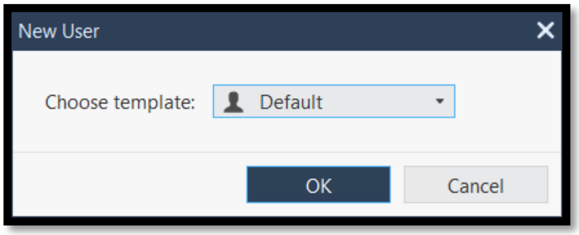
In the previous exercises, we configured various method of acquiring a user identity and use it for the security policy enforcement.

In this exercise, we will configure an external contractor who will get to access the streaming application YouTube. However, this user is not user created on the Domain Controller. We will create an internal user account in SmartConsole to grant this contractor access.

1. Create a new internal user in SmartConsole.
   a. New -> More -> User/Identity -> User



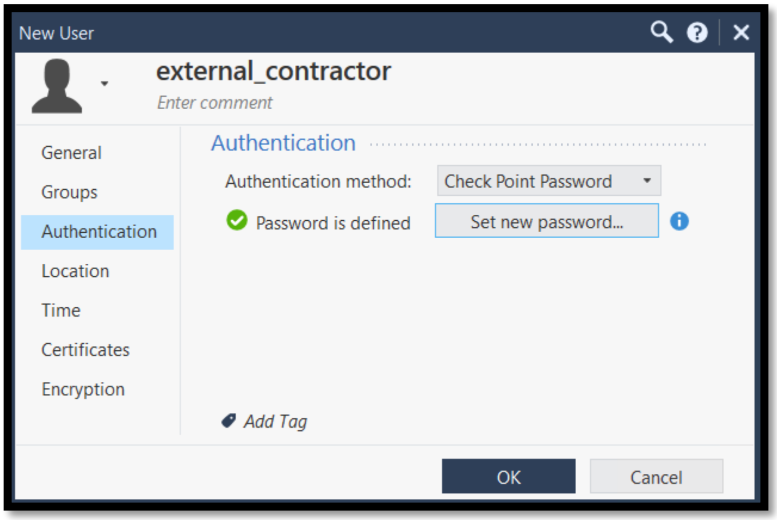
2. Select the default user template.



New User

Choose template: Default

3. Give this user a name and configure the authentication as Check Point Password and set a proper password.



New User

external_contractor

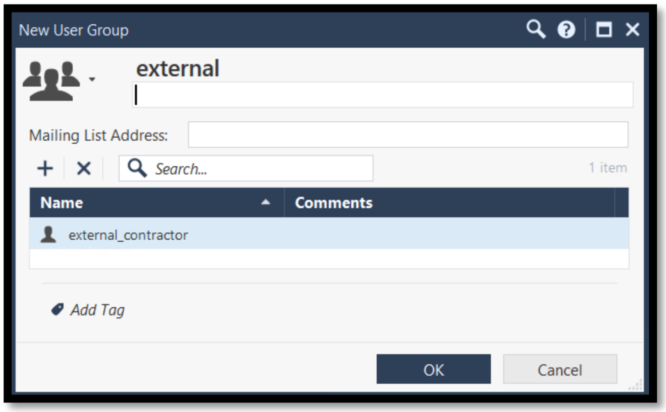
*Enter comment*

Authentication

Authentication method: Check Point Password

Password is defined

4. Add a new user group and add the user we created above to this group.
   a. New -> More -> User/Identity -> User Group

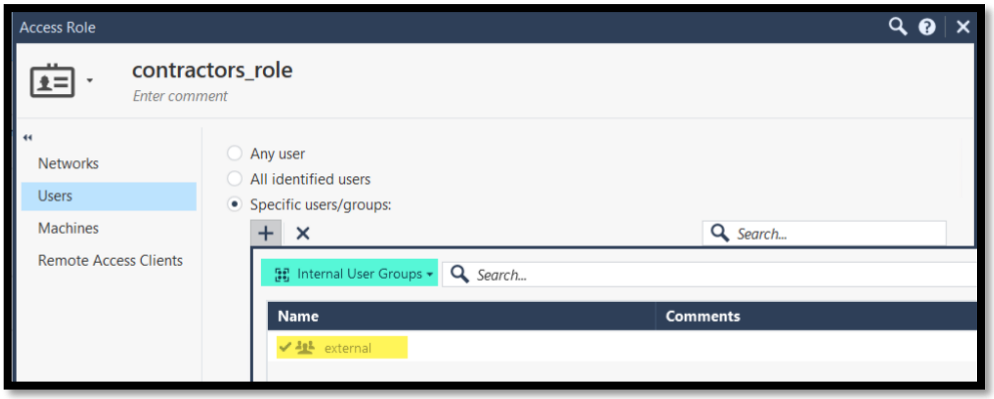


external

Mailing List Address:

| Name | Comments |
|---|---|
| external_contractor | |

5. A Create a new Access Role and give it a proper name and add the new external User Group we created earlier.
   - Note that you need to change the default filter to be able to see Internal User Groups

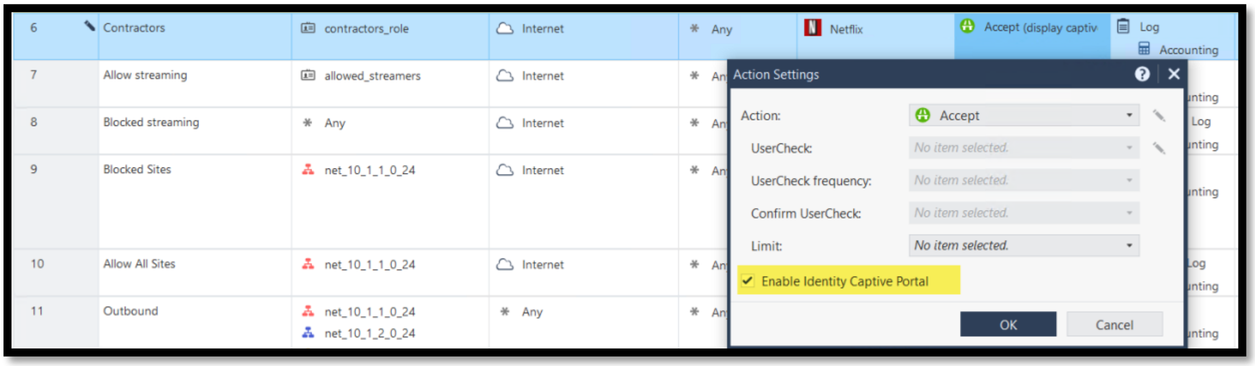


contractors_role

○ Any user
○ All identified users
● Specific users/groups:

| Name | Comments |
|---|---|
| ✓ external | |

6. Create a new rule on top of the rule allowing YouTube. This rule will allow the contractors_role to access Netflix.
   - Note that we will need to modify the Action column to enable the Identity Captive Portal via More –> Action Settings. See below.



|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| 6 | Contractors | contractors_role | Internet | Any | Netflix | Accept (display captiv | Log<br>Accounting |
| 7 | Allow streaming | allowed_streamers | Internet | An |  |  | unting |
| 8 | Blocked streaming | Any | Internet | An |  |  | Log<br>unting |
| 9 | Blocked Sites | net_10_1_1_0_24 | Internet | An |  |  | unting |
| 10 | Allow All Sites | net_10_1_1_0_24 | Internet | An |  |  | Log<br>unting |
| 11 | Outbound | net_10_1_1_0_24<br>net_10_1_2_0_24 | Any | An |  |  | unting |

Action Settings

Action: Accept

UserCheck: No item selected.

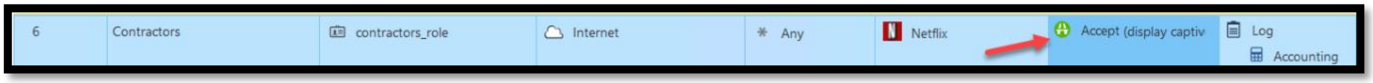
UserCheck frequency: No item selected.

Confirm UserCheck: No item selected.

Limit: No item selected.

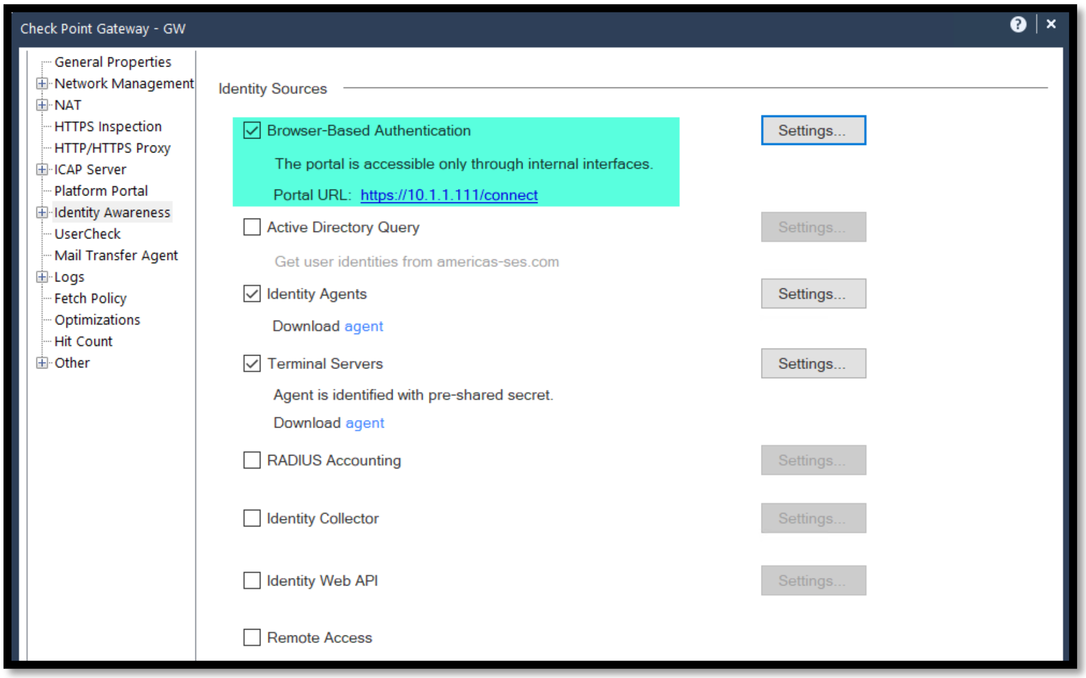
☑ Enable Identity Captive Portal

7. Confirm the final rule looks as expected.



|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| 6 | Contractors | contractors_role | Internet | Any | Netflix | Accept (display captiv | Log<br>Accounting |

8. Edit the GW object and enable the browser-based Authentication



Check Point Gateway - GW

Identity Sources

☑ Browser-Based Authentication

The portal is accessible only through internal interfaces.

Portal URL: https://10.1.1.111/connect

☐ Active Directory Query

Get user identities from americas-ses.com

☑ Identity Agents

Download agent

☑ Terminal Servers

Agent is identified with pre-shared secret.

Download agent

☐ RADIUS Accounting

☐ Identity Collector

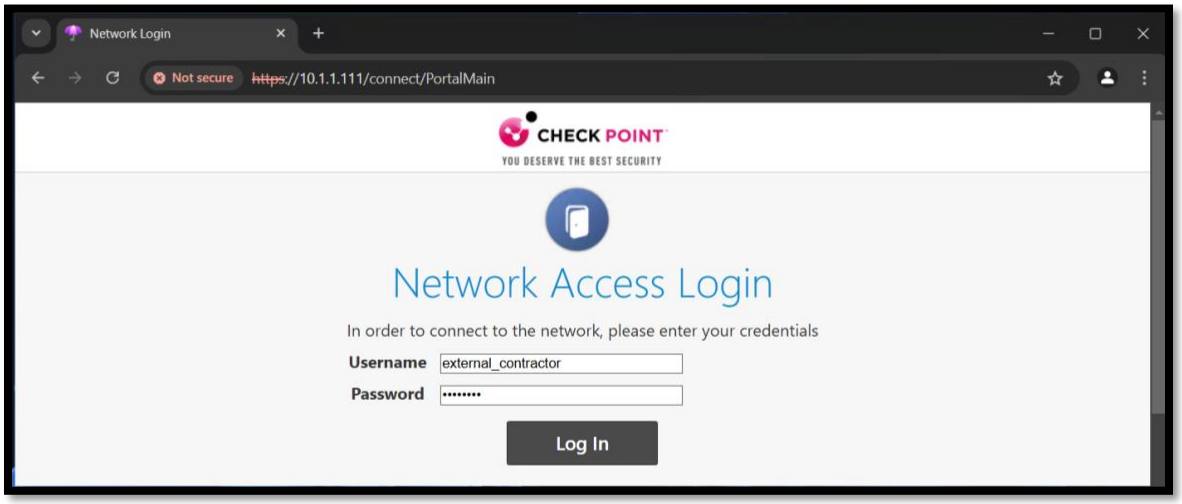
☐ Identity Web API

☐ Remote Access

- Note that the external user is unknown to the GW. The user will be redirected to the Identity captive portal to provide the credentials.

9. Sign in to the windows client using the preconfigured RDP session for the local admin account.

10. Open chrome and try to reach Netflix. Note that you are being forwarded to the Identity Captive Portal. Provide the credentials of the **external_contractor**.



Network Login

Not secure ~~https~~://10.1.1.111/connect/PortalMain

CHECK POINT
YOU DESERVE THE BEST SECURITY

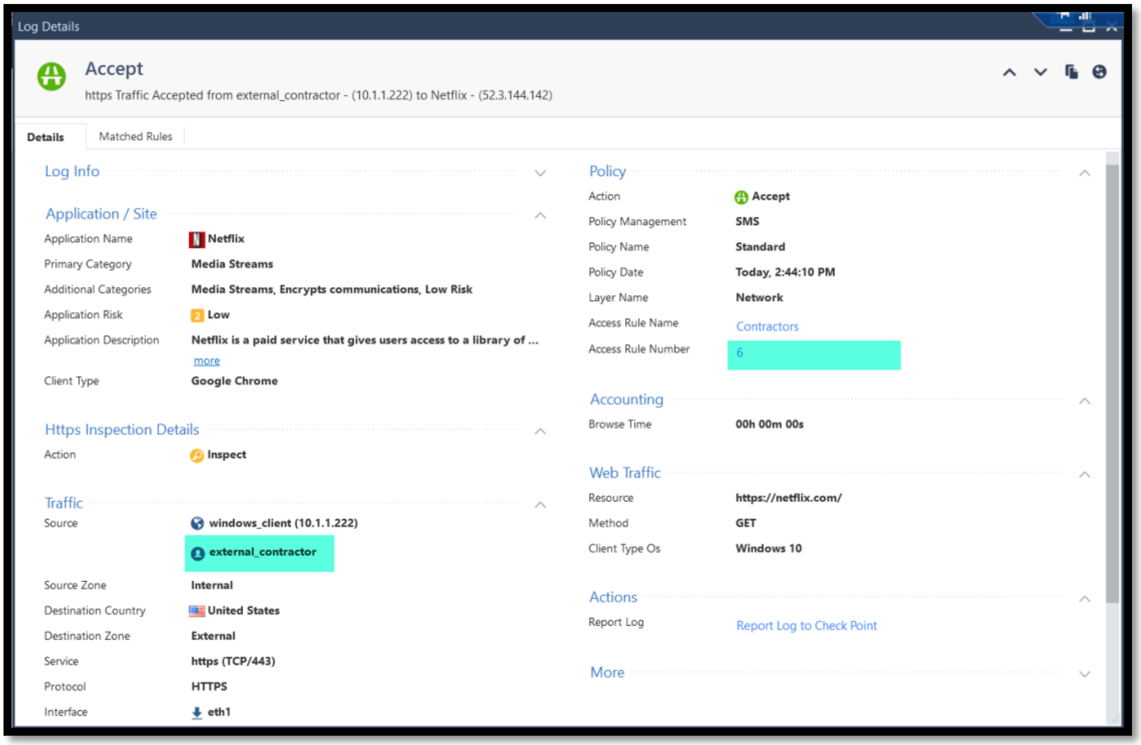
Network Access Login

In order to connect to the network, please enter your credentials

| | |
|---|---|
| Username | external_contractor |
| Password | •••••••• |

Log In

11. Once the identity is provided and the GW can confirm that the user is allowed to reach Netflix based on rule 6. Review the logs and confirm.



Log Details

Accept
https Traffic Accepted from external_contractor - (10.1.1.222) to Netflix - (52.3.144.142)

Details | Matched Rules

Log Info

Application / Site

| | |
|---|---|
| Application Name | Netflix |
| Primary Category | Media Streams |
| Additional Categories | Media Streams, Encrypts communications, Low Risk |
| Application Risk | 2 Low |
| Application Description | Netflix is a paid service that gives users access to a library of ...<br>more |
| Client Type | Google Chrome |

Https Inspection Details

| | |
|---|---|
| Action | Inspect |

Traffic

| | |
|---|---|
| Source | windows_client (10.1.1.222)<br>external_contractor |
| Source Zone | Internal |
| Destination Country | United States |
| Destination Zone | External |
| Service | https (TCP/443) |
| Protocol | HTTPS |
| Interface | eth1 |

Policy

| | |
|---|---|
| Action | Accept |
| Policy Management | SMS |
| Policy Name | Standard |
| Policy Date | Today, 2:44:10 PM |
| Layer Name | Network |
| Access Rule Name | Contractors |
| Access Rule Number | 6 |

Accounting

| | |
|---|---|
| Browse Time | 00h 00m 00s |

Web Traffic

| | |
|---|---|
| Resource | https://netflix.com/ |
| Method | GET |
| Client Type Os | Windows 10 |

Actions

| | |
|---|---|
| Report Log | Report Log to Check Point |

More

End of Lab 3