Identity Awareness

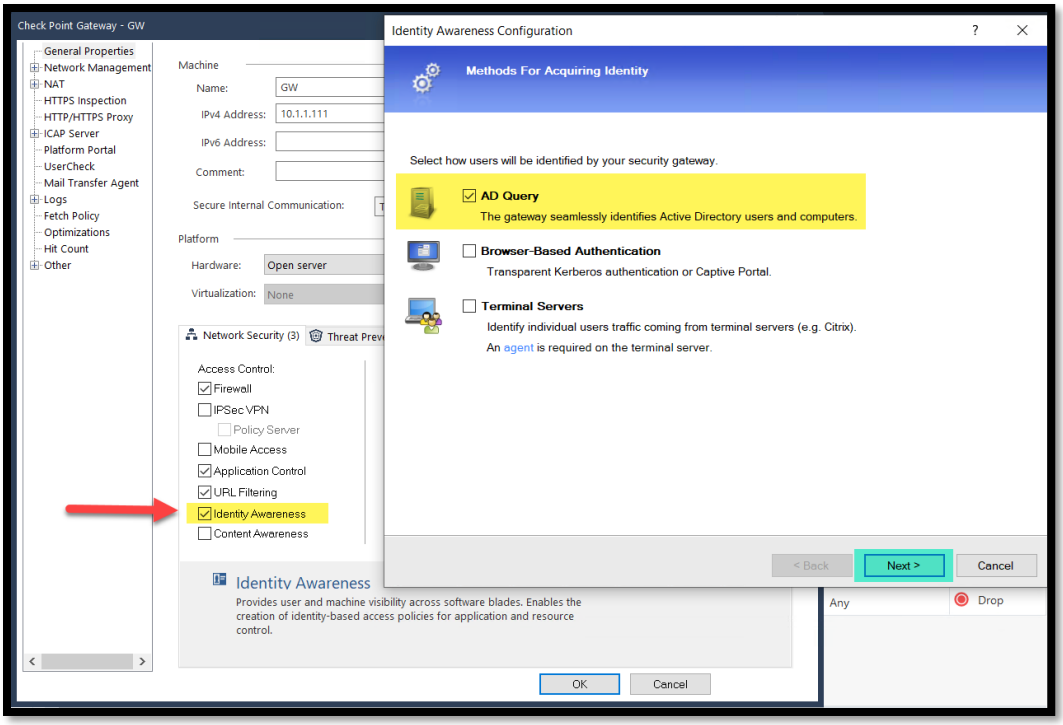
Introduction

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

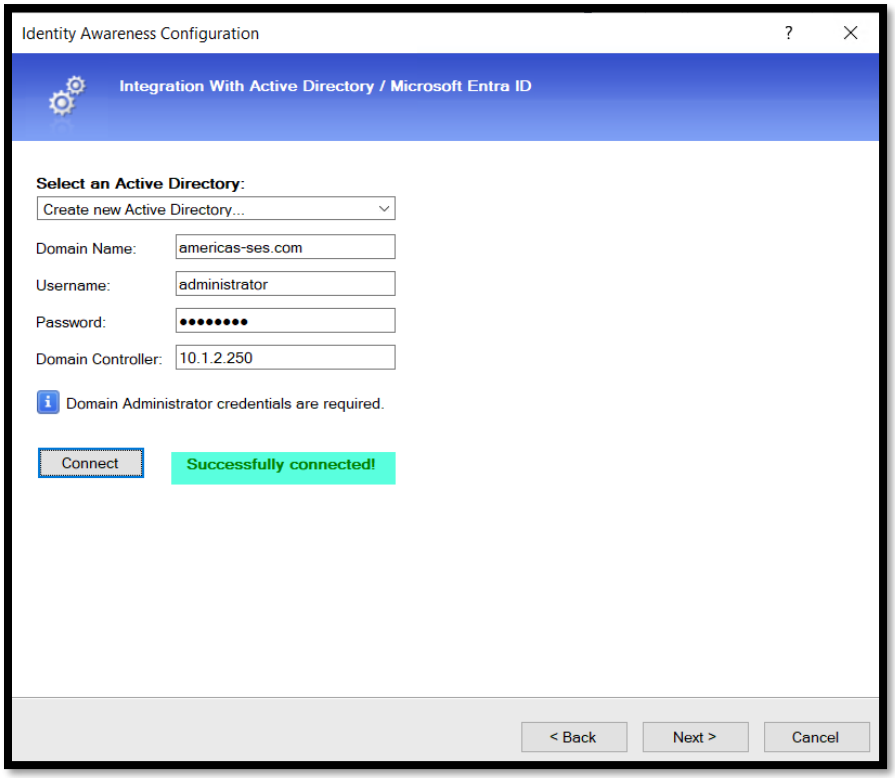
ADQuery is an easy to configure, clientless tool to get identities. Its function is based on Active Directory integration, and it is fully transparent to the user.

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

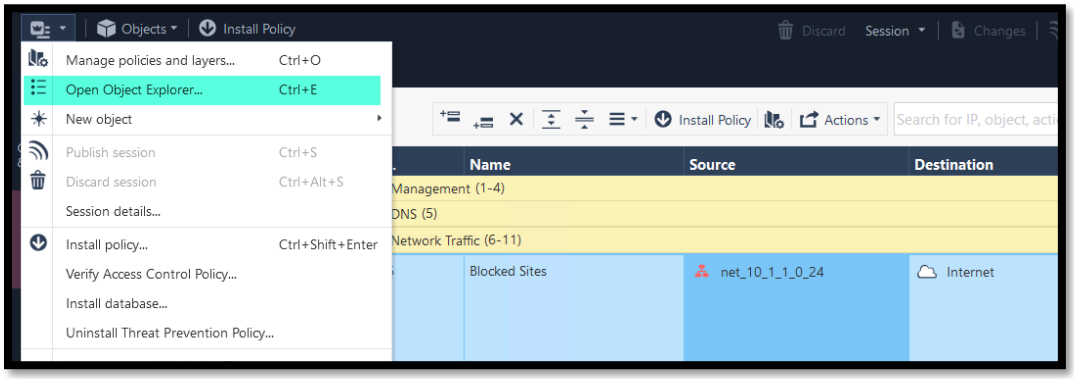


2. Fill in the required Active Directory details and click **Connect**. Make sure the connection is successful and finish the configuration wizard and close the GW object.

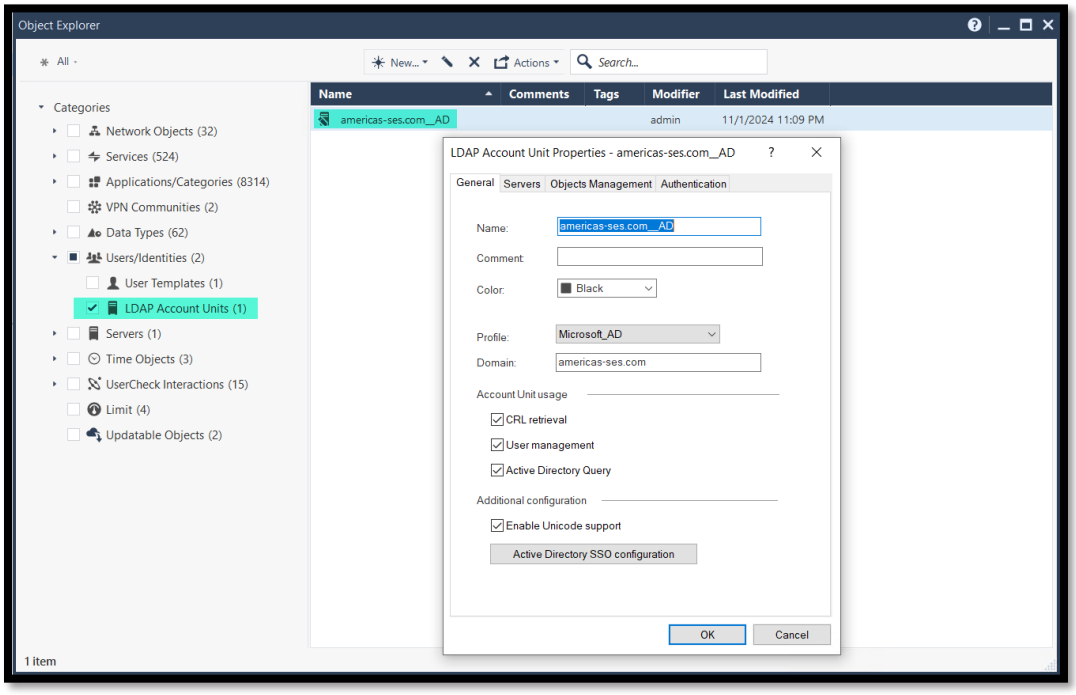
Domain Name	americas-ses.com
Username	administrator
Password	Cpwins!1
Domain Controller	10.1.2.250



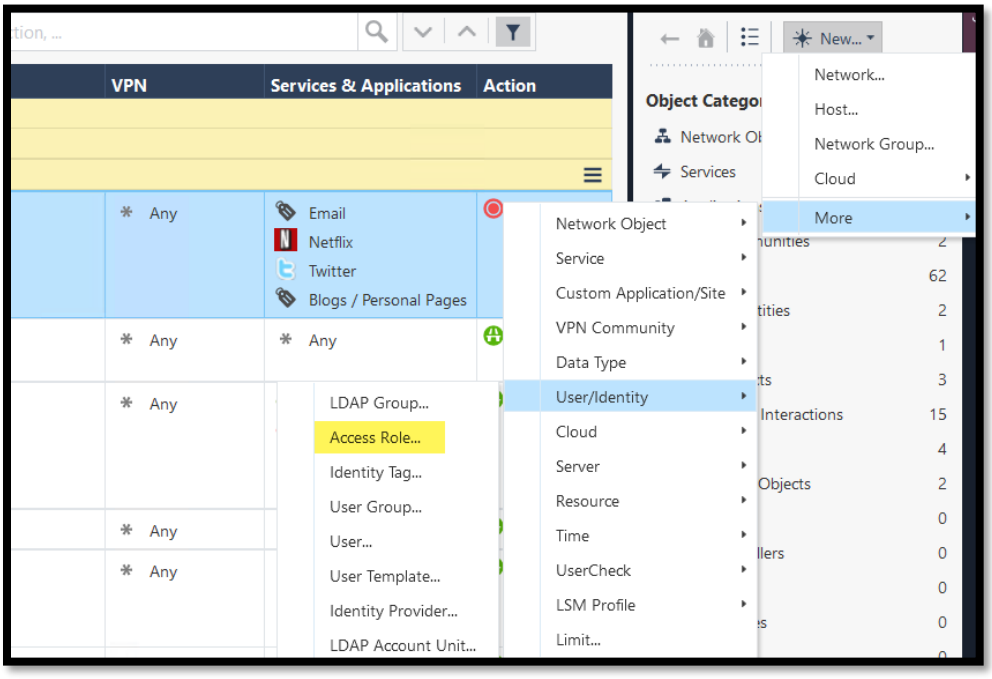
3. The wizard above creates an Account unit object. This object contains all configurations related the active directory. Open the Object Explorer.



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

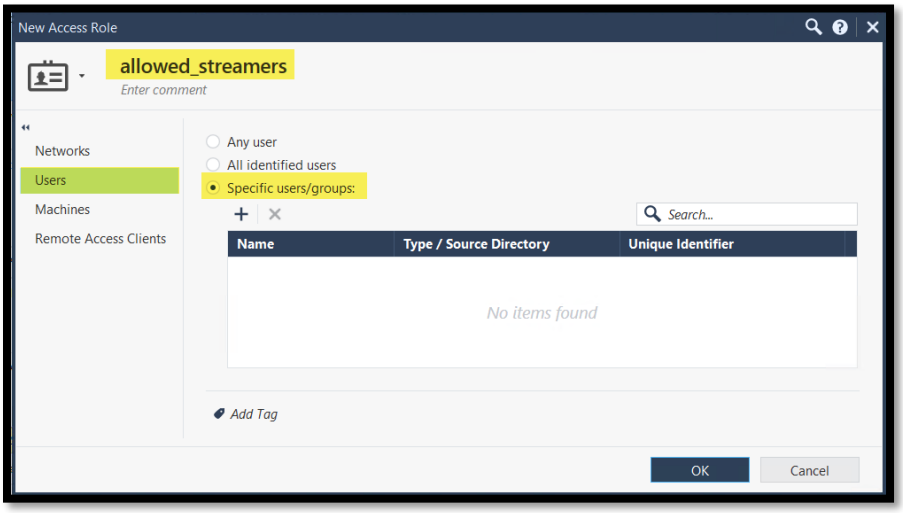


5. Create a new Access Role (New -> More -> User/Identity -> Access Role).

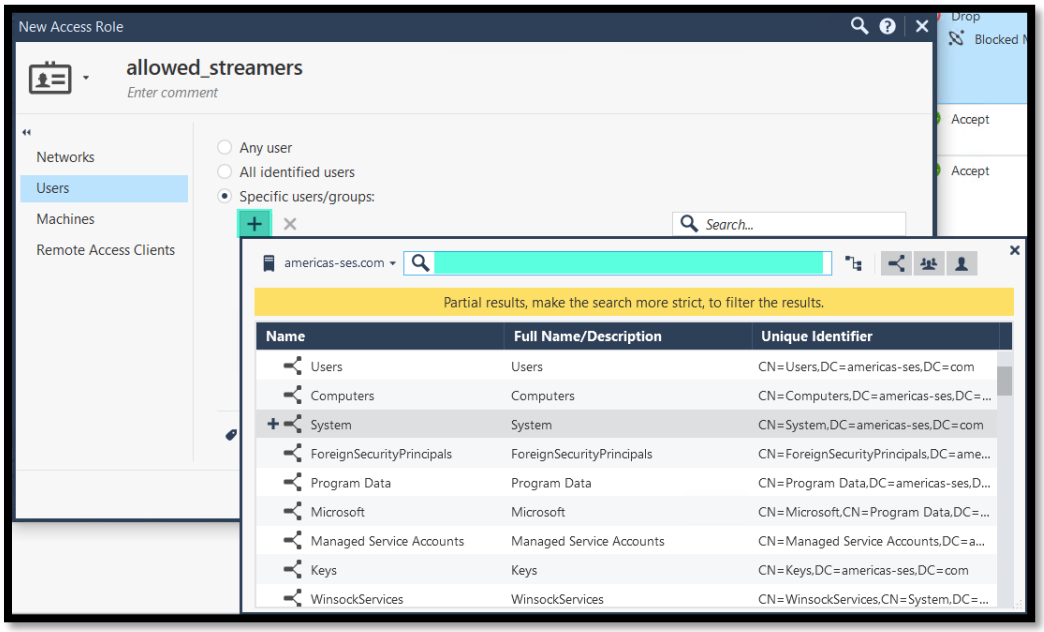


- You can use Access Role objects as source and/or destination parameter in a rule. Access Role objects can include one or more of these objects:
  - Networks
  - Users and user groups
  - Computers and computer groups
  - Remote Access clients

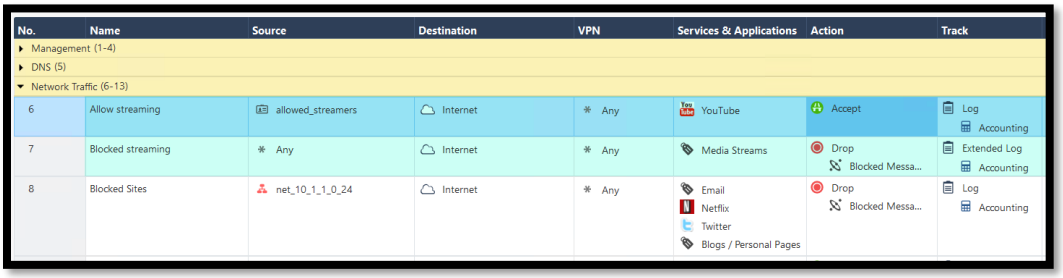
6. We will create rules to block all media streaming applications and allow it to one specific group of users. Give the object a proper name and select the Users - > Specific users/groups.



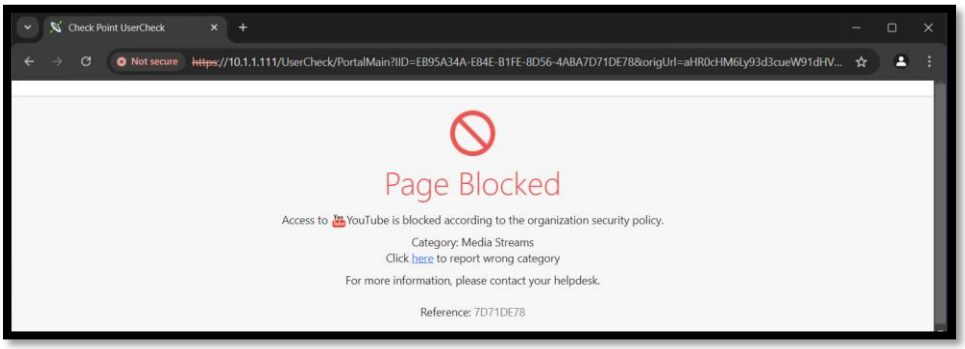
7. Click (+) and notice that the object explorer is showing the users and identities from the domain controller windows-server at 10.1.2.250.



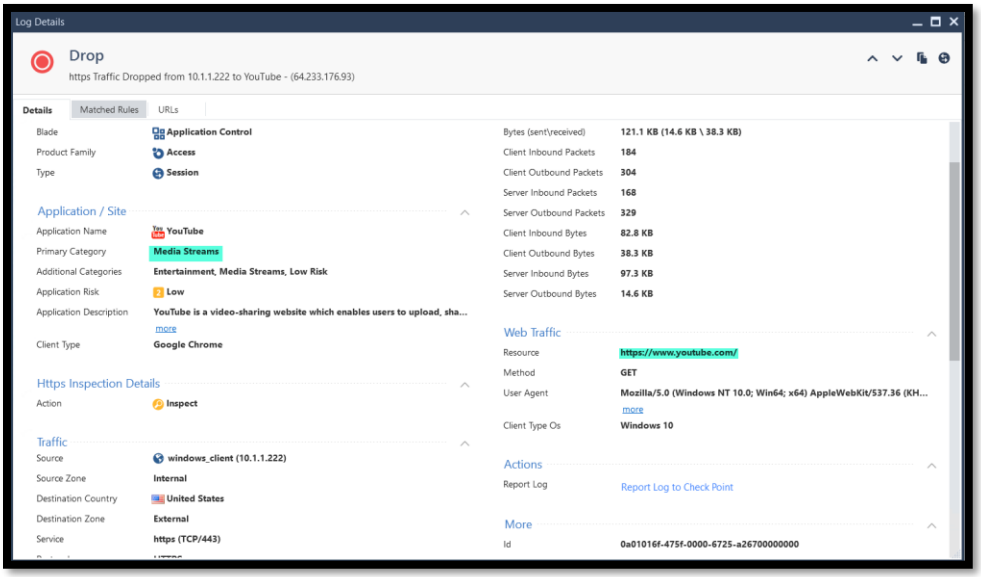
8. Create two new rules on top of the Blocked sites rule. The rule above allows the users from the access role we created earlier (t1_admin) is allowed to access YouTube. The rule below it will block access to all Media Steaming sites including YouTube to everyone else.



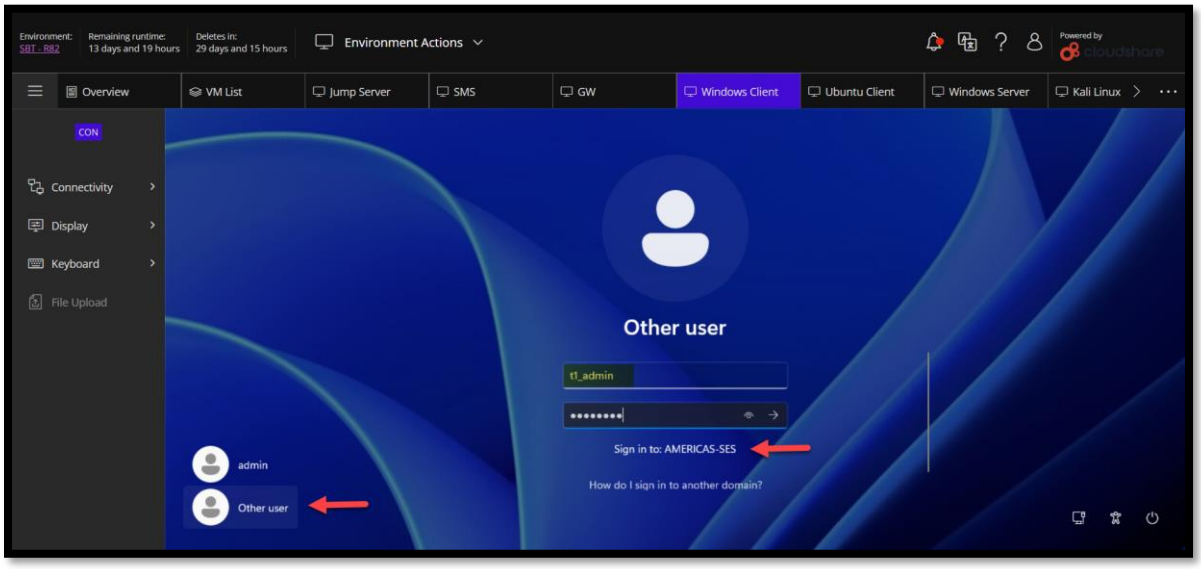
9. Install the access policy.
10. Login to the win-client host and test reaching YouTube. It should be blocked based on rule 7.
    - You are logged in using a local account (admin).



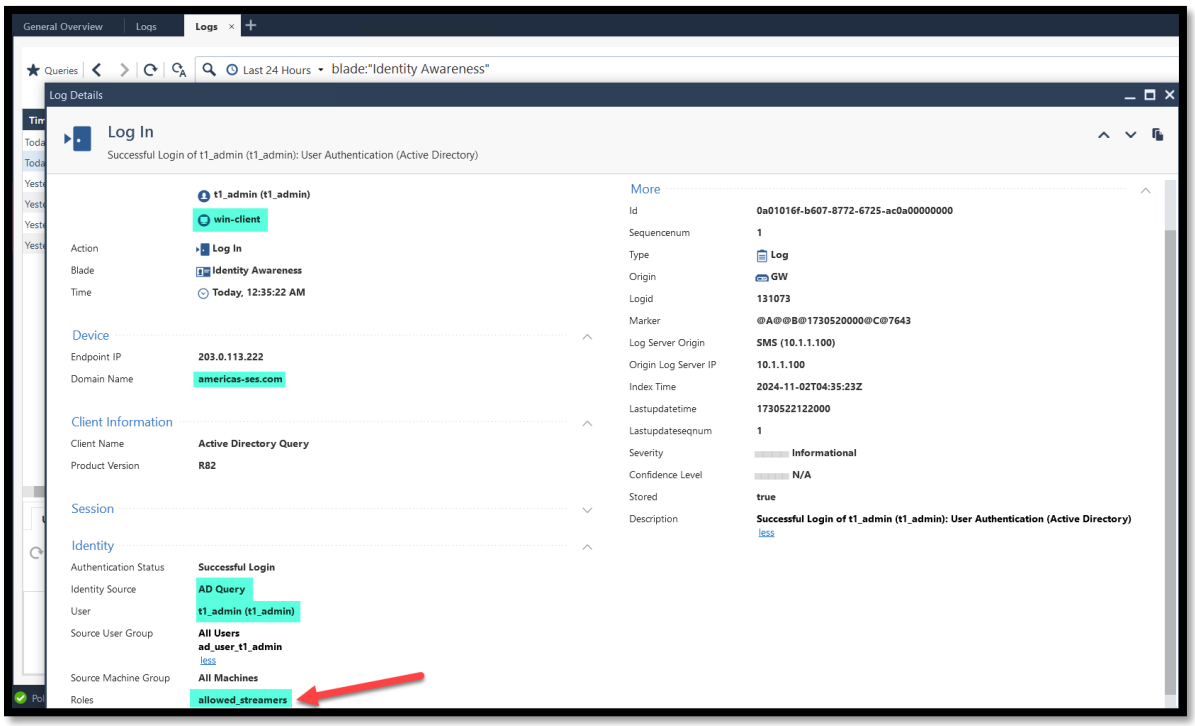
11. Review the logs and confirm that the traffic was blocked by the correct rule.



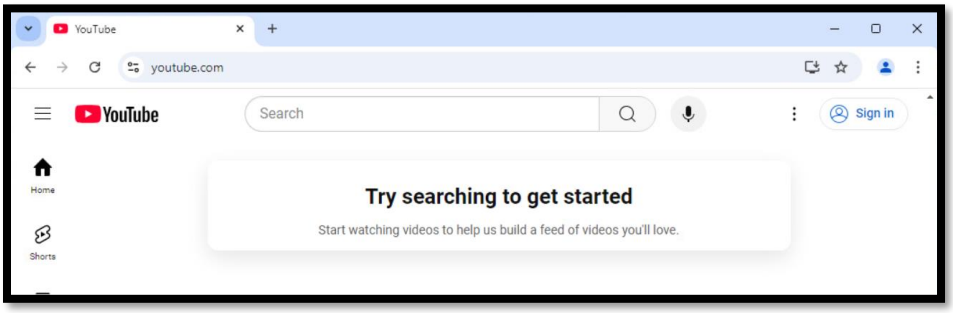
12. From the class environment, select the **Windows Client** host and login as t1_admin/Cpwins!1
    - Note that this user is part of the access rule we created earlier, and it is allowed to reach YouTube.
    - The machine below is part of the domain (Americas-ses.com). The login will create an event 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).



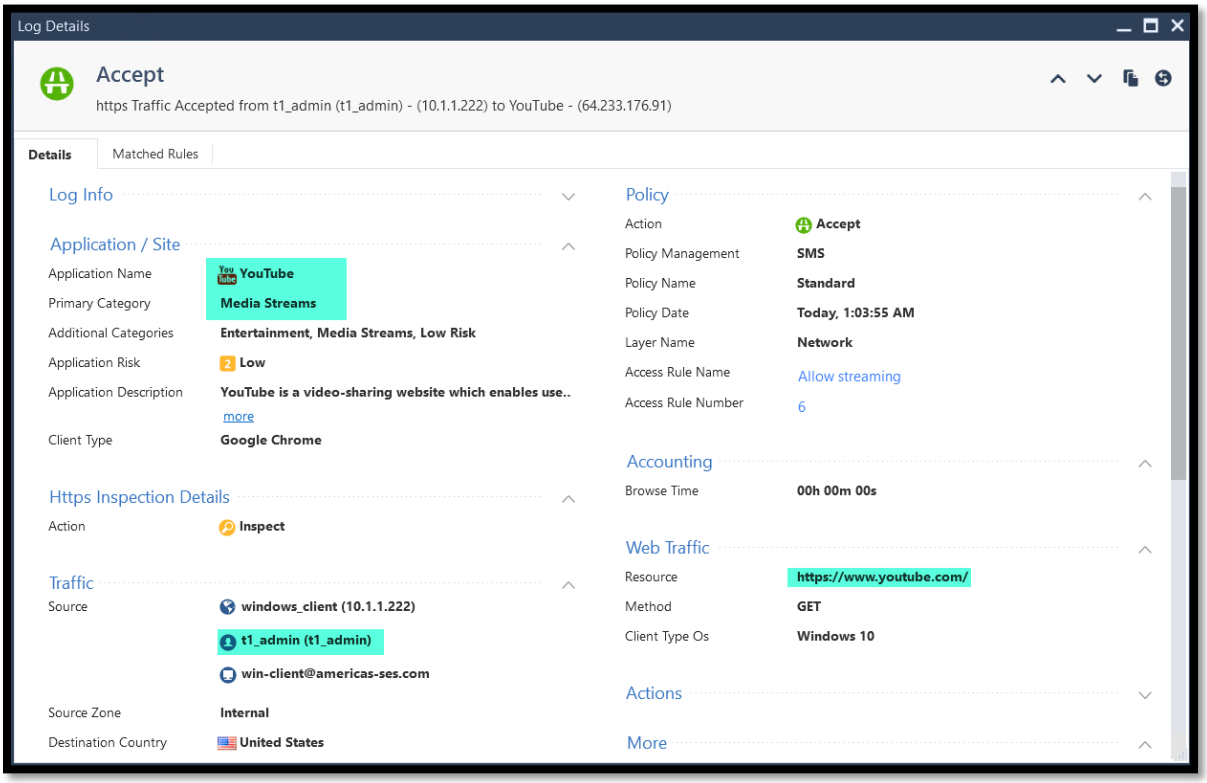
13. Filter the logs to see Identity Awareness related logs. Notice that the user identity was acquired correctly and that the Access Role was associated to this user.



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



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



16. 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.
```

17. To see all discovered identities based on the AD events, run the command (adlog a query user all).
    - Note that this tool allows a short format. You can use 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;
```

18. 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
********************************************************************************
```

19. 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).

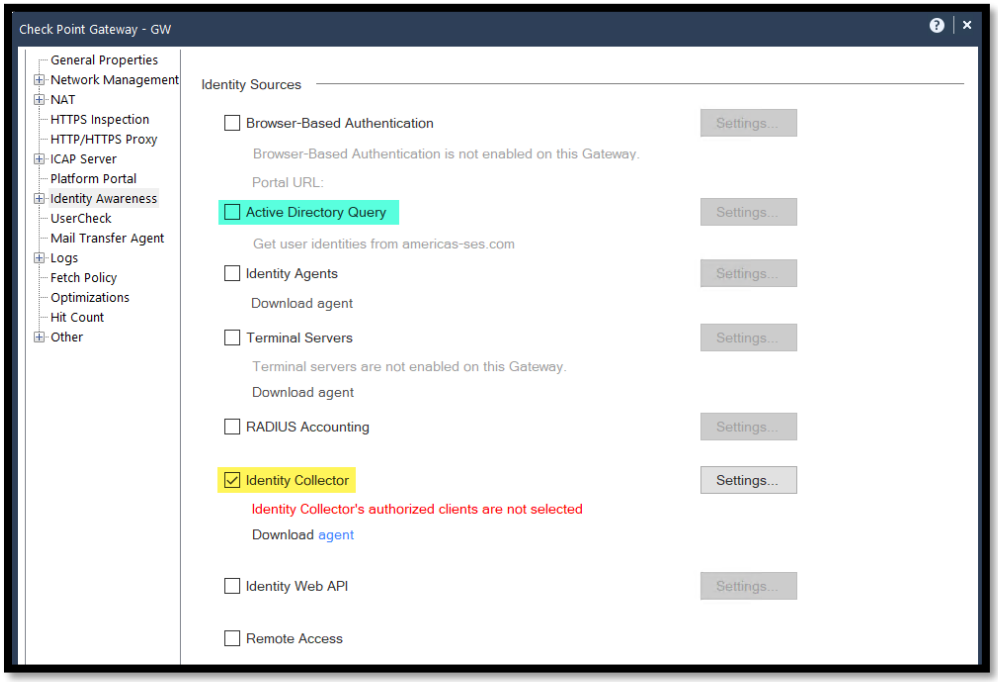

```
[Expert@GW:0]# pep show user a
Command: root->show->user->all
ID (PDP; UID)                        Username@Machine                CID (IP, PacketID)          PT
=============================================================================================================
127.0.0.1      :00000000; 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

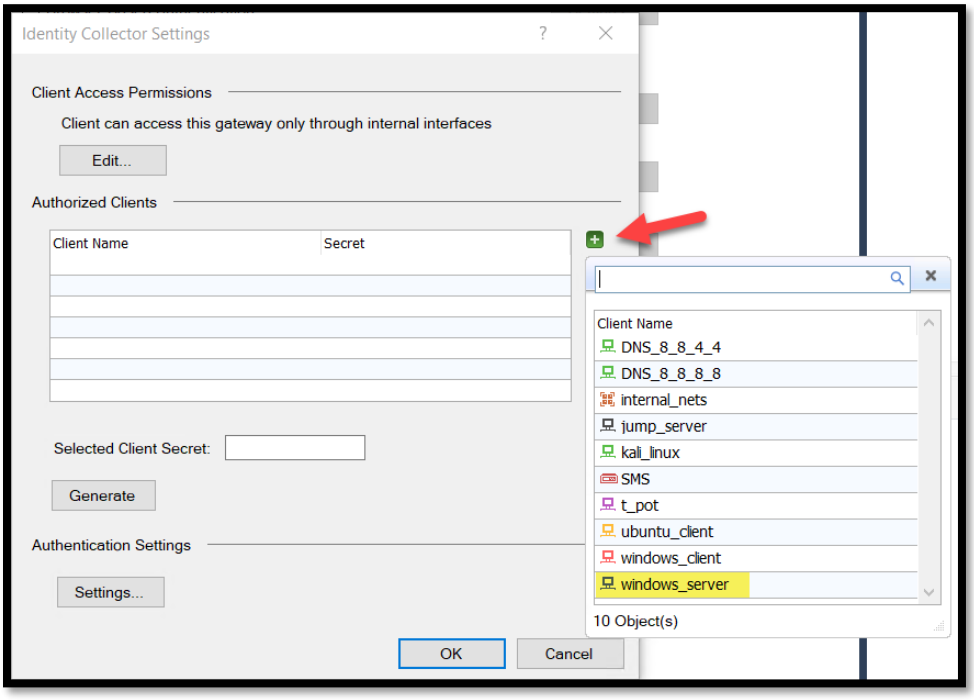
ADQuery uses WMI processes on the domain controller. There is performance degradation related to this design. To solve this problem among other issues, Check Point developed a new tool called Identity Collector.

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.

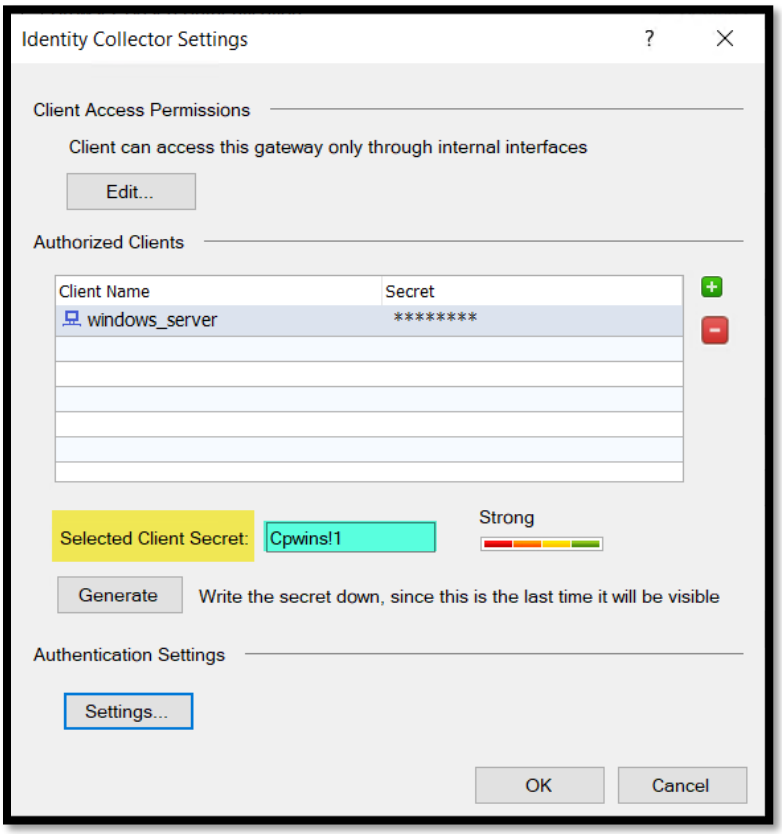
1. Edit the GW object and uncheck **Active Directory Query** and enable **the Identity Collector**.



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

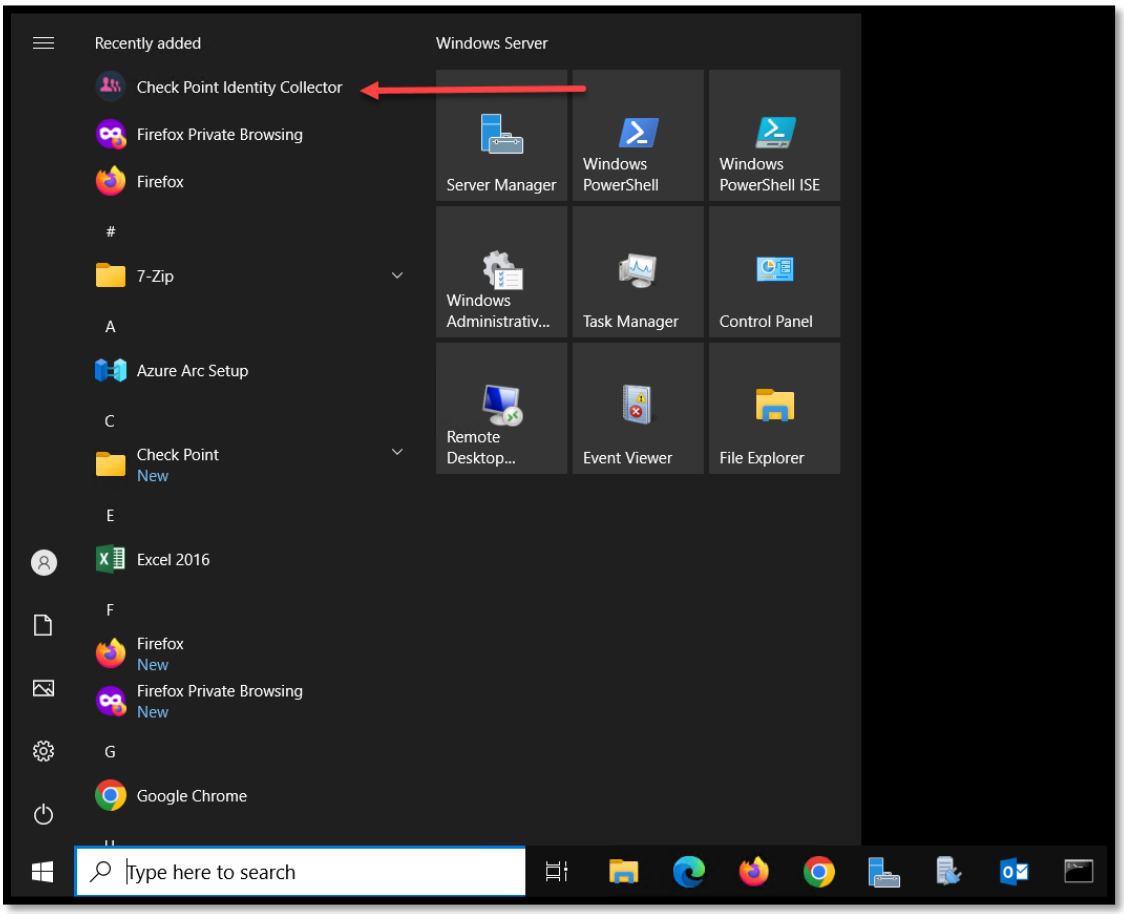


3. Keep the generated client secret or type one manually. We will use this code later.

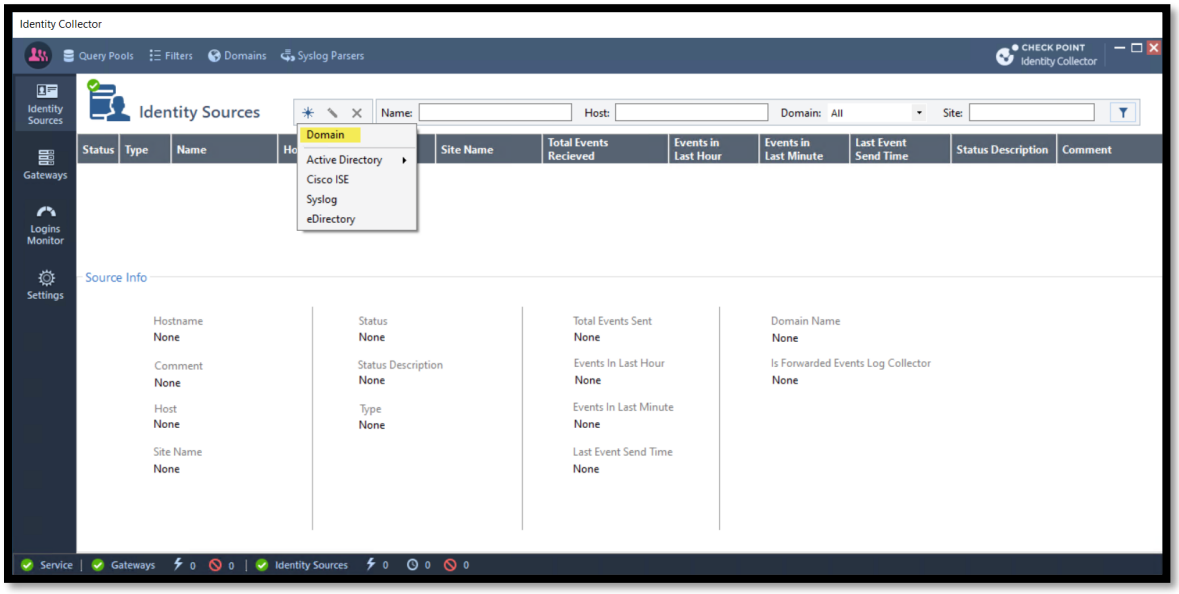


4. Click OK to return to the Identity Sources configurations. Click on the link to download the Identity Collector Agent.
   - https://support.checkpoint.com/results/sk/sk1343

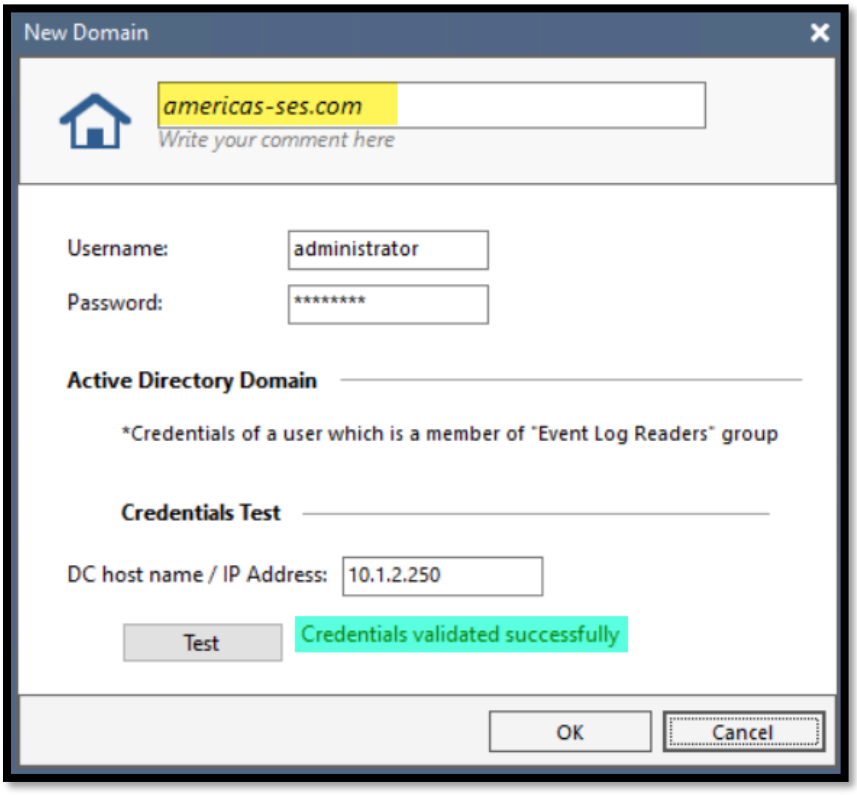
5. While the file is downloading, **Install the Access Policy**.
6. Copy the installation file to the Windows Server and install the agent.
7. Open the Identity Collector tool.



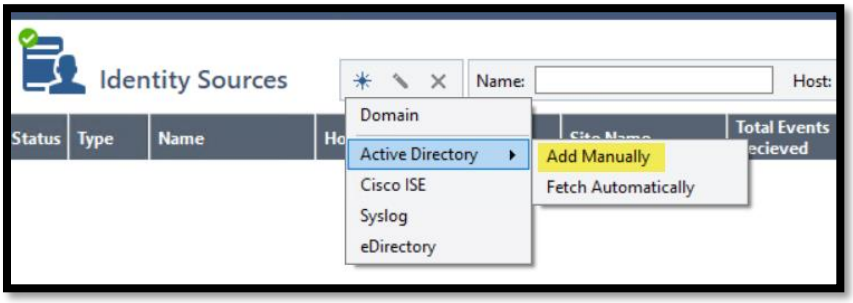
8. While in the default Identity Sources tab, add a new domain.



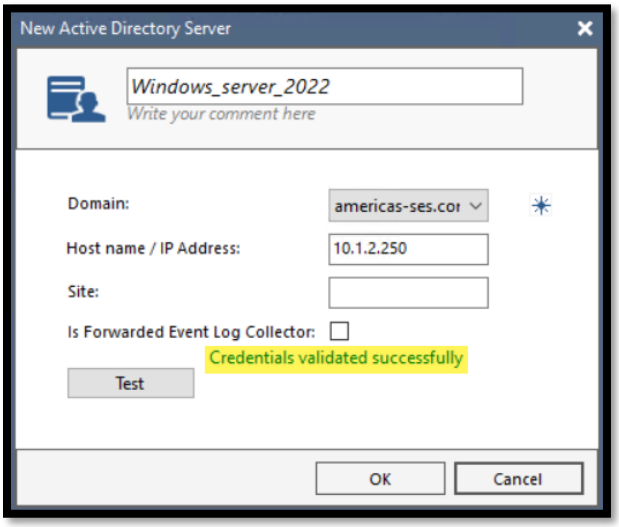
9. Provide the Domain Controller details. Test the credentials and click OK.



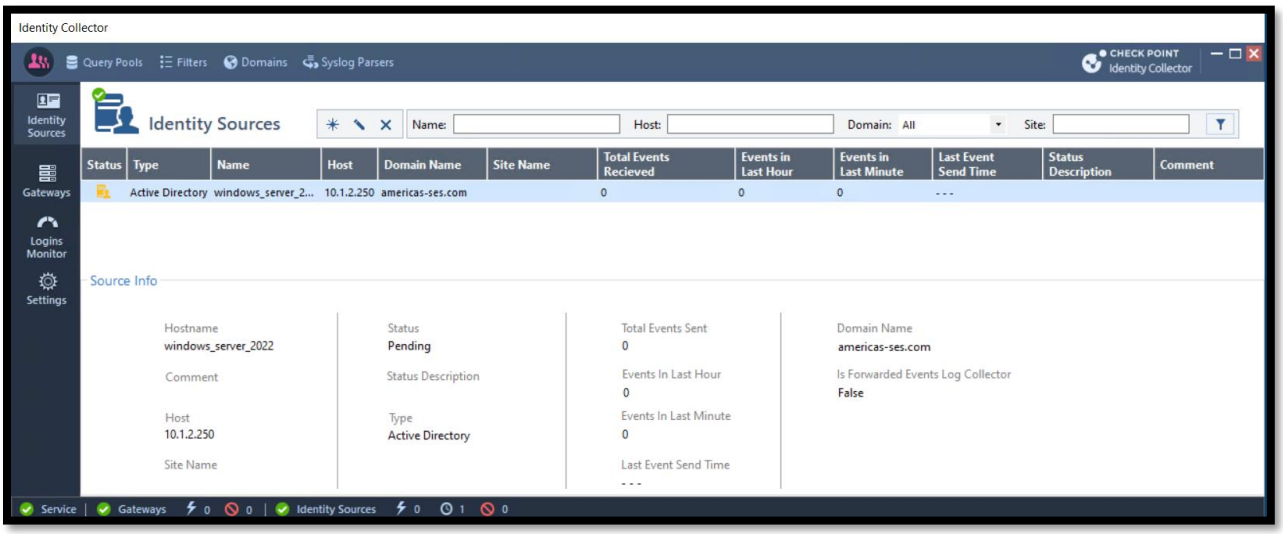
10. Add a new Active Directory manually.



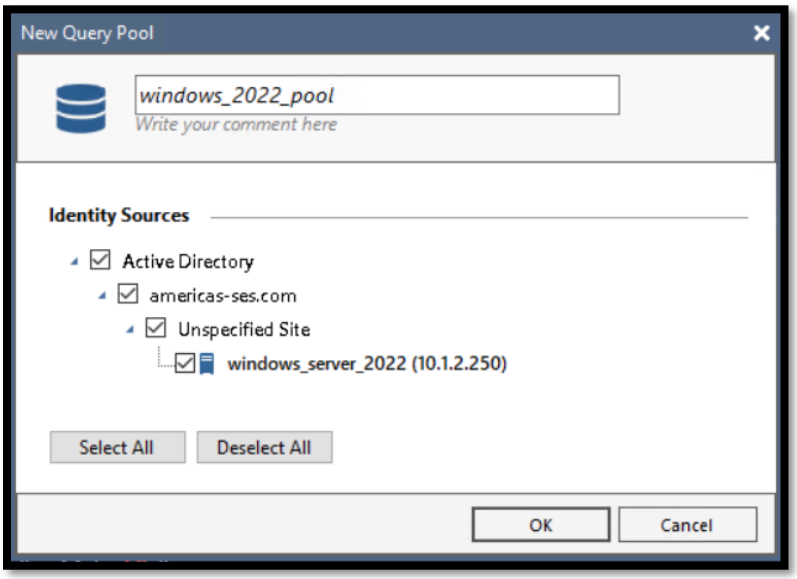
11. Provide the details and test the connection and click OK to exit the window.



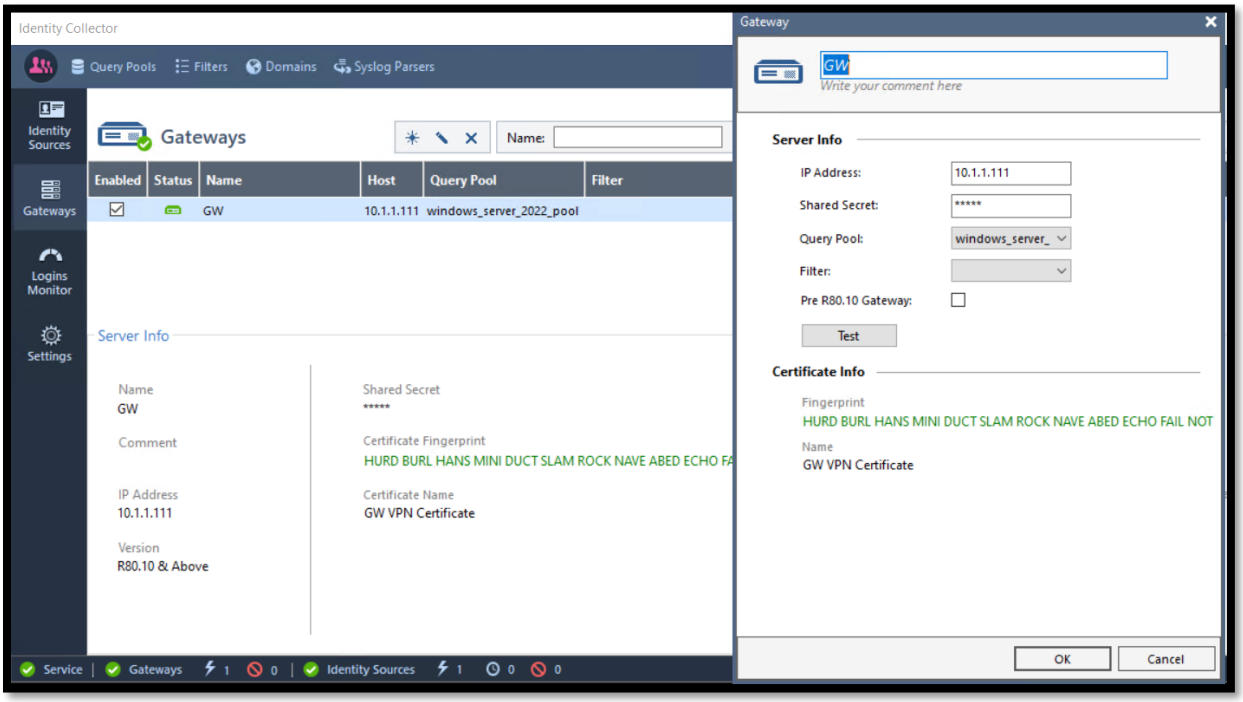
12. By this stage, the identity collector is configured to collect logs from the domain controller of the domain Americas-ses.com



13. Create a new Query pool. This pool decided which events are forwarded to which GW.

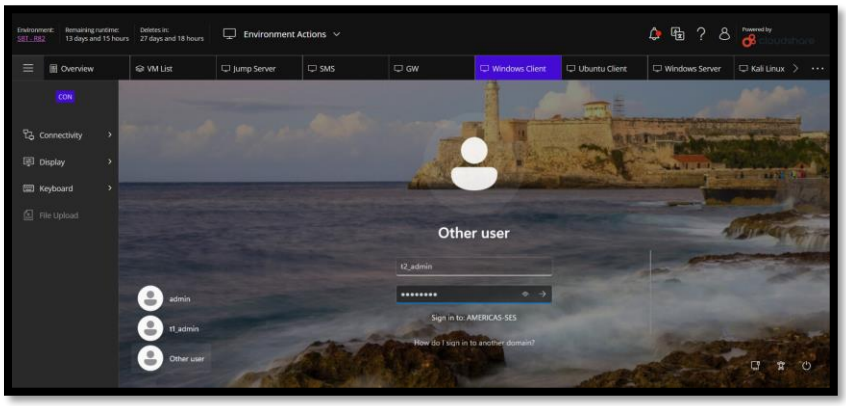


14. Move to the Gateway section, add a new Gateway configuration. Use the secret we configured on the GW object in SmartConsole earlier.

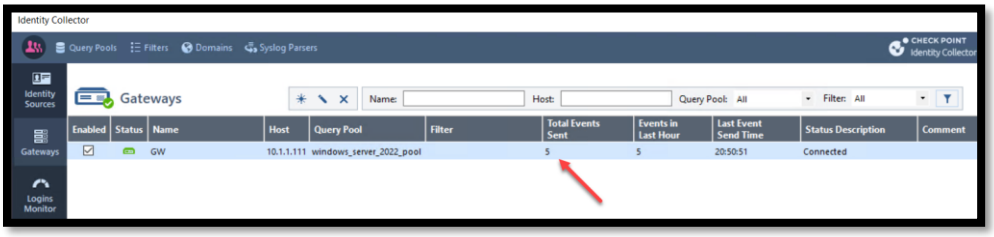


- Notice that the self-signed certificate is presented. **Trust** it to complete the setup.
- We will not use filters, but we need to specify the query pool we created in the previous step.

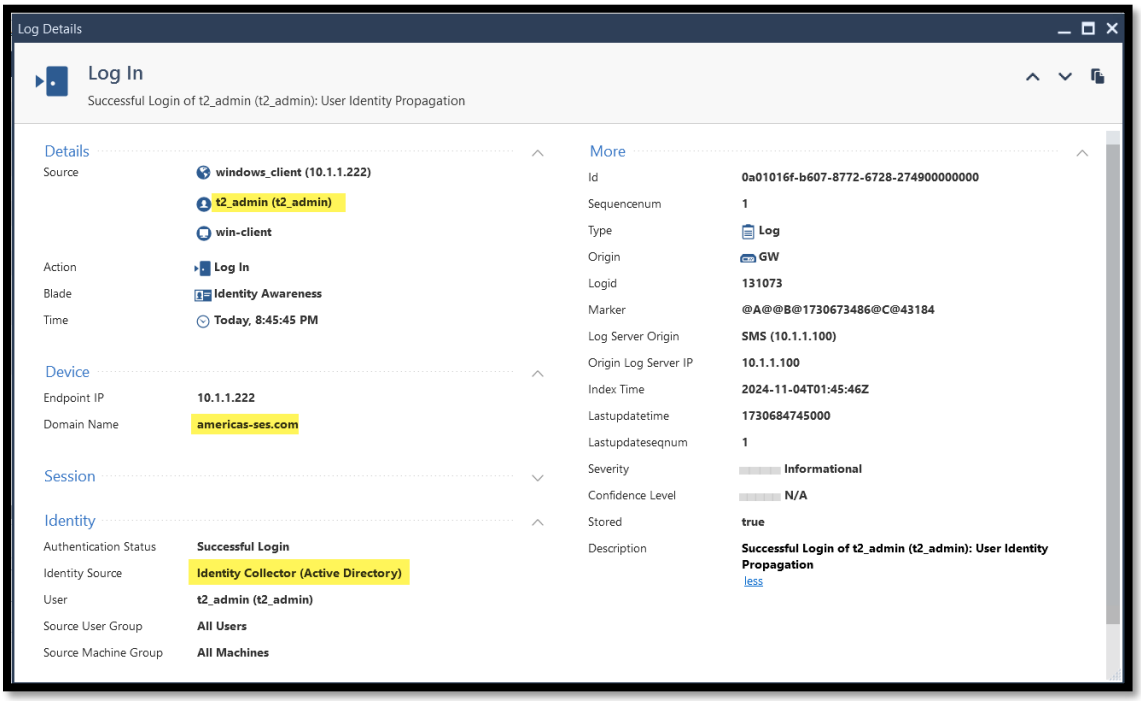
15. Generate a login from the windows client machine. Login as t2_admin



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



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



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

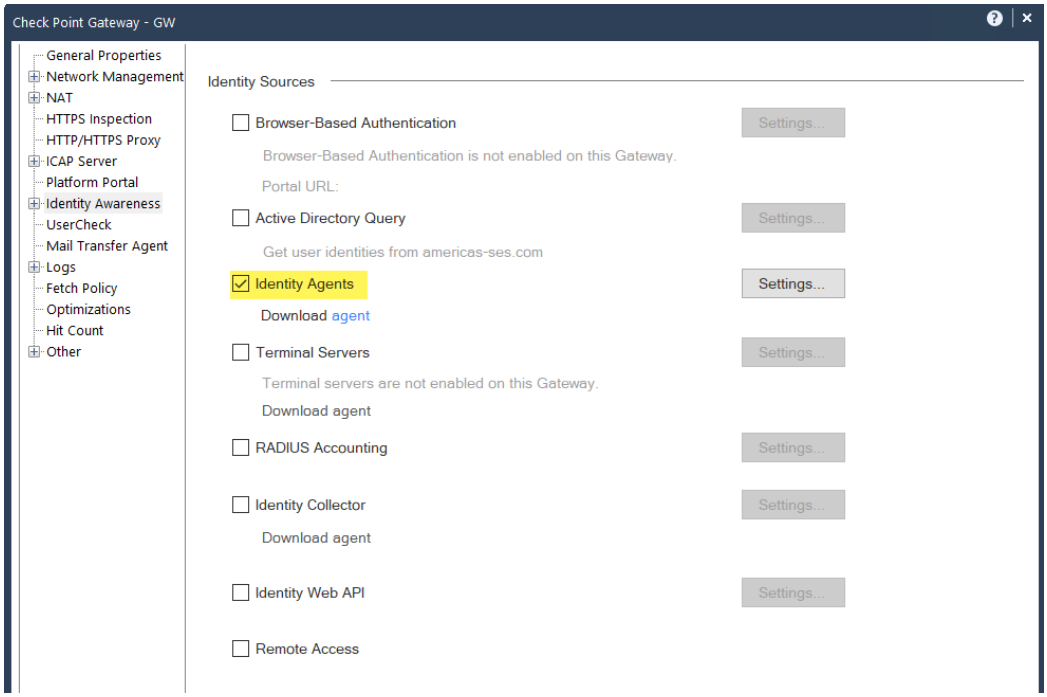
```
[Expert@GW:0]# pdp m u a

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: -
```

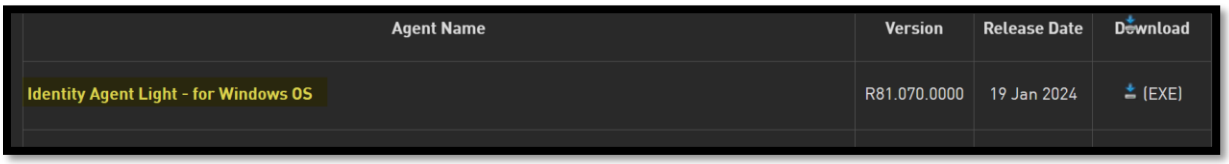
Exercise 3: Identity Agents

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.

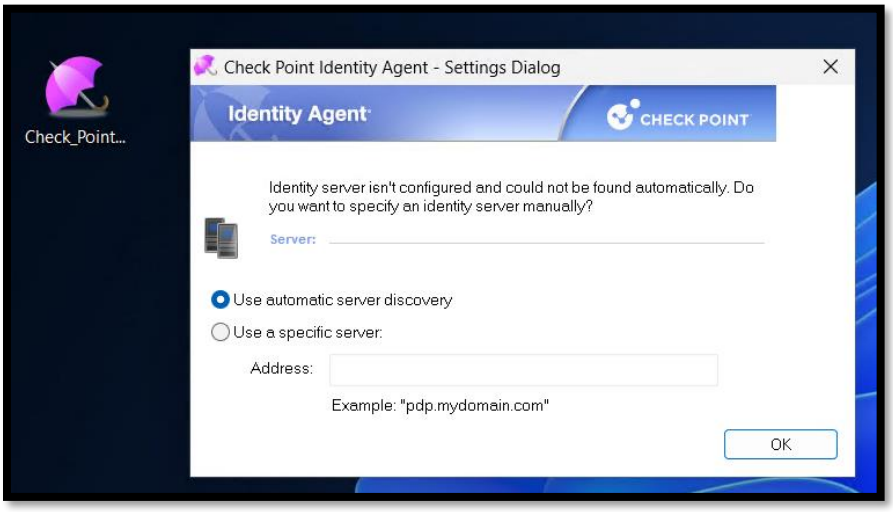
1. Edit the GW object and Enable the Identity Agent and disable the Identity Collector.



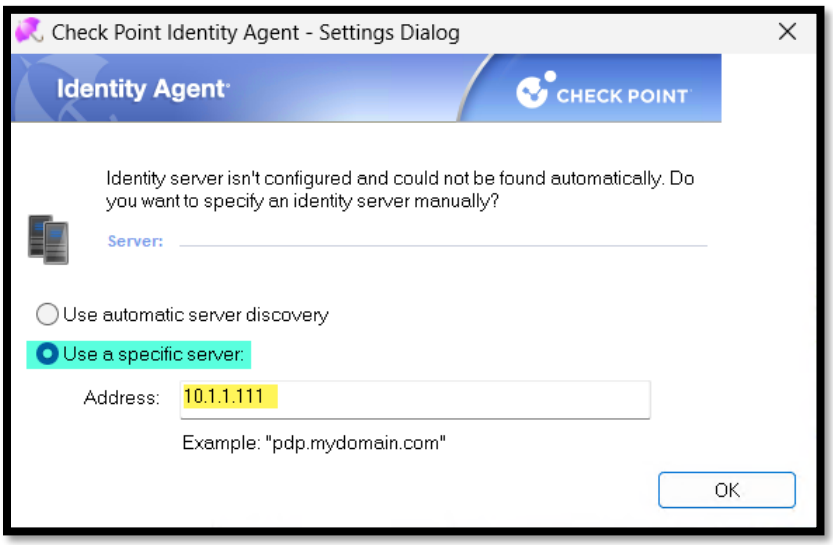
2. Download the lightweight agent via the link. This is the same SK where we downloaded the Identity Collector. All other clients are also available for download.



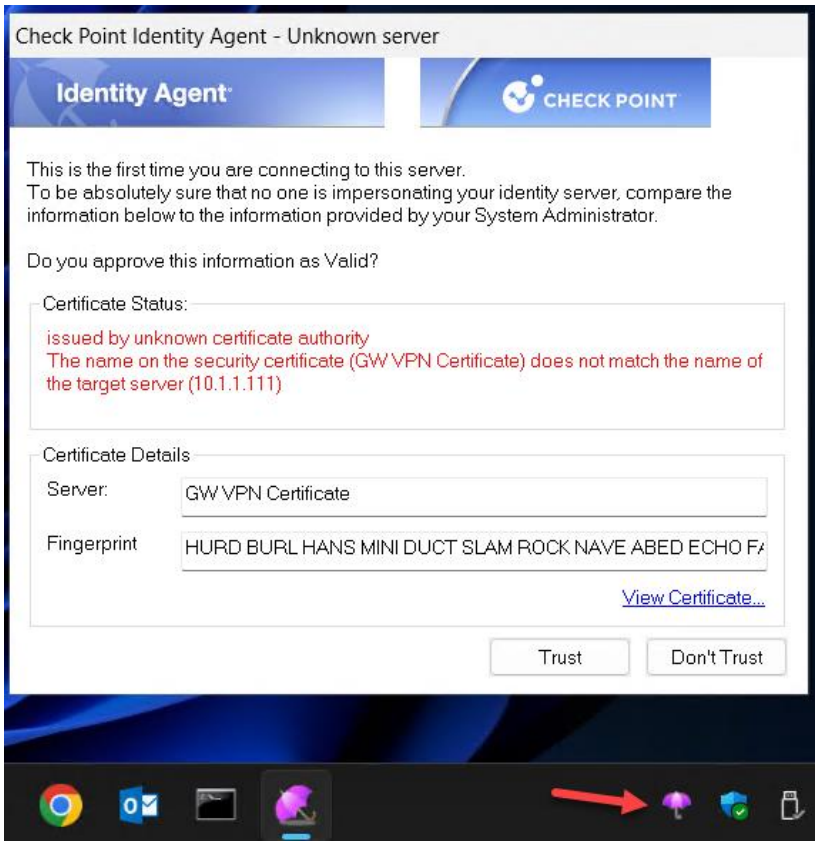
3. Log in to the windows client machine over RDP. The saved session on the Jump Server desktop is configured with the **local** account *admin/Cpwins!1* which is not a domain user. Copy and Install the identity agent we just downloaded.



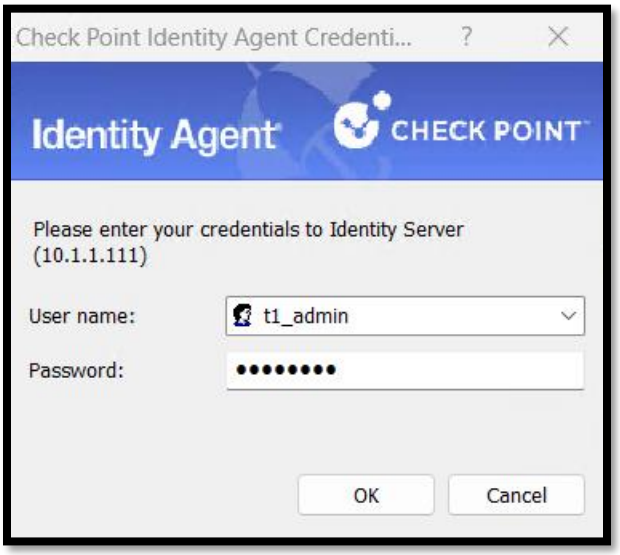
4. Select Use a specific server and provide the GW IP address and click OK.



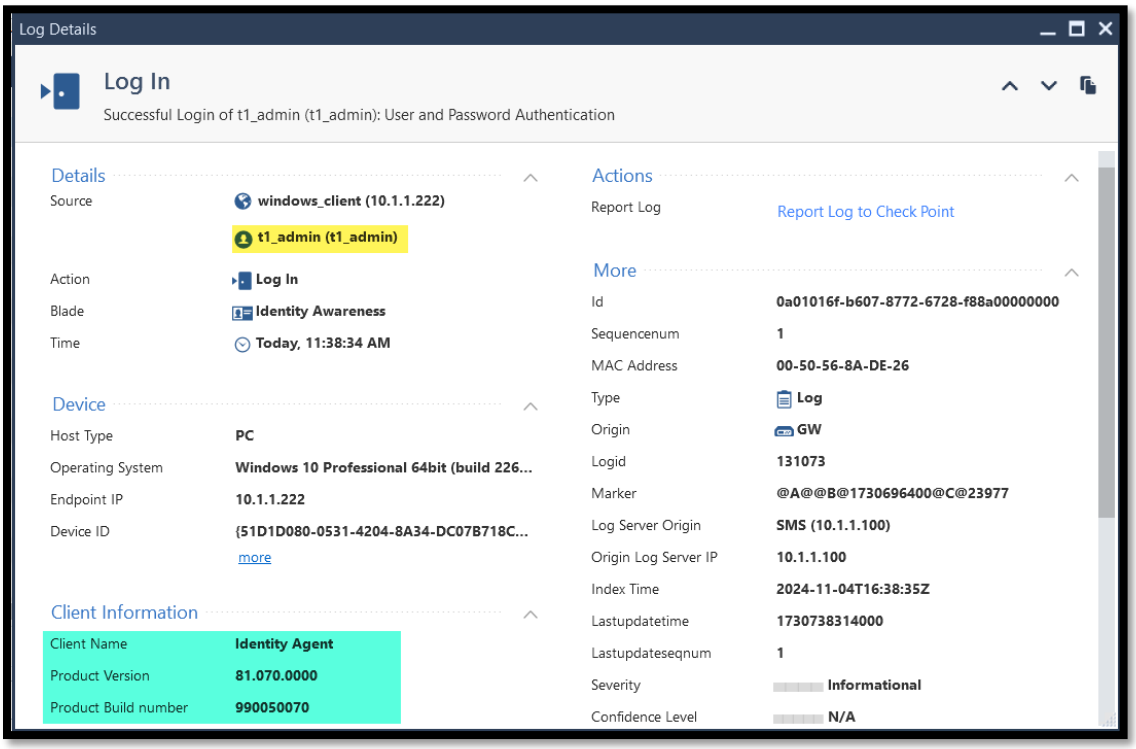
5. Like connecting via the identity collector, the Agent is presented with the default VPN certificate. Trust it and continue.



6. 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.



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



8. 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
```

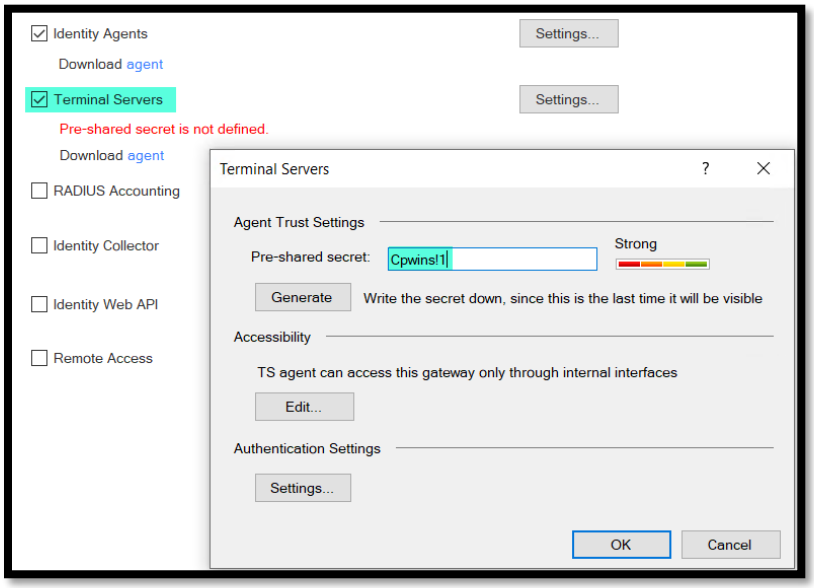
9. Try to reach YouTube and review the logs to confirm the traffic was allowed by the correct rule.

Exercise 4: Terminal Servers Agent (MuH)

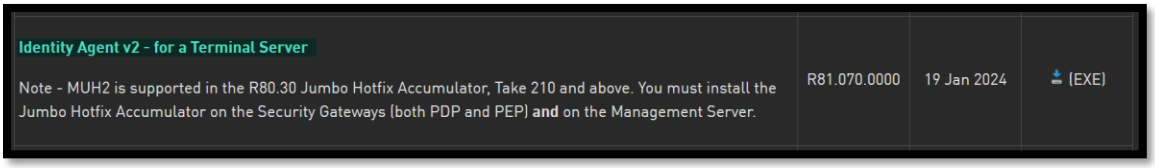
In the previous exercise, we used the Check Point identity agent to grant a user access. This will handle the authentication single user. There are different deployment scenarios where multiple users are using the same machine such as in terminal servers.

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

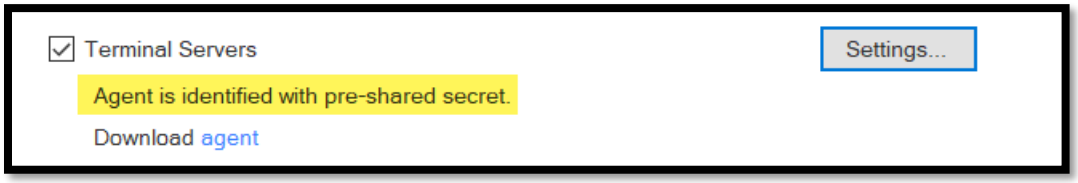
1. Edit the GW object, Enable Terminal Servers. And click Settings to configure the Pre-shared secret.



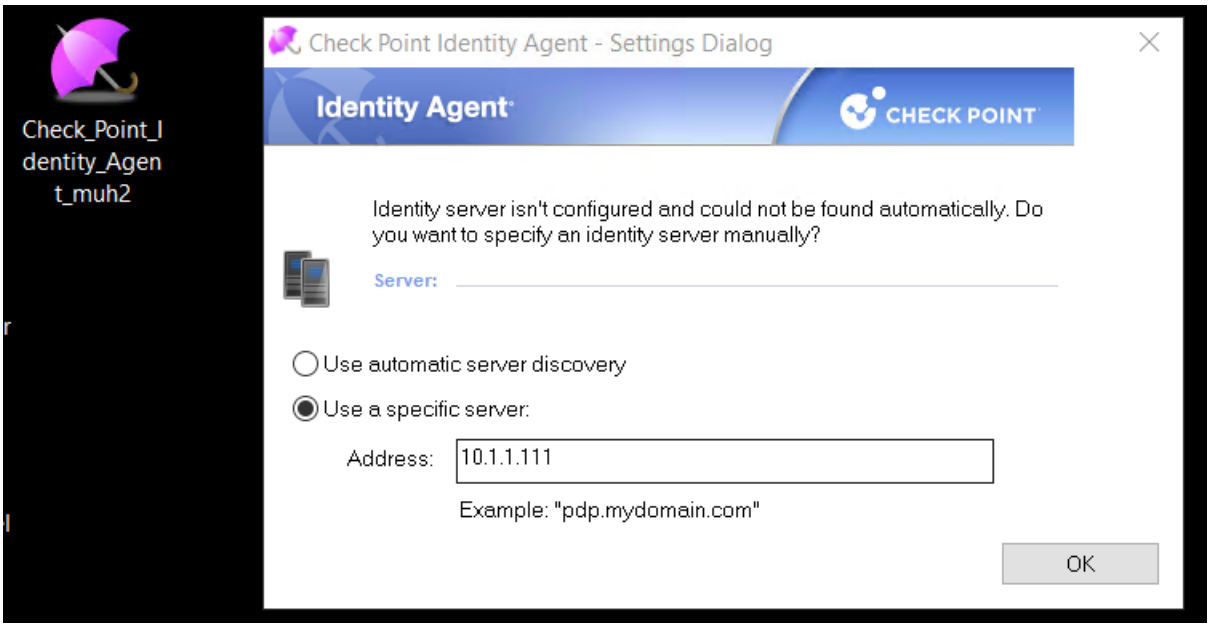
2. Download the Identity Agent v2 for terminal servers. Use the same SK we used to download the previous clients.



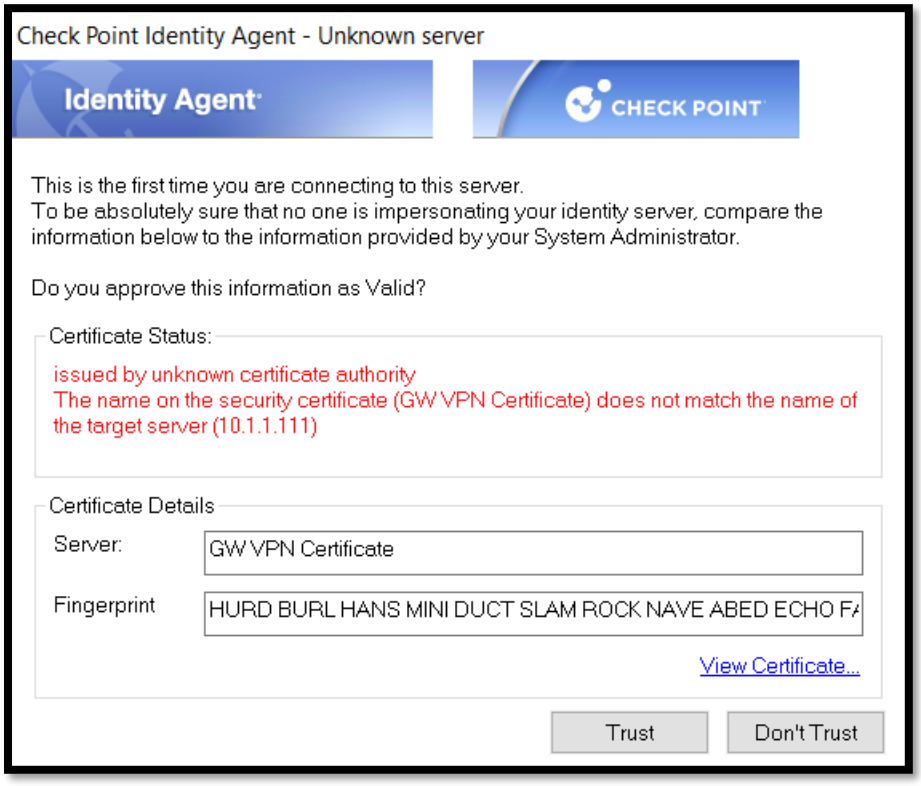
3. Confirm the secret is confired and install the access policy.



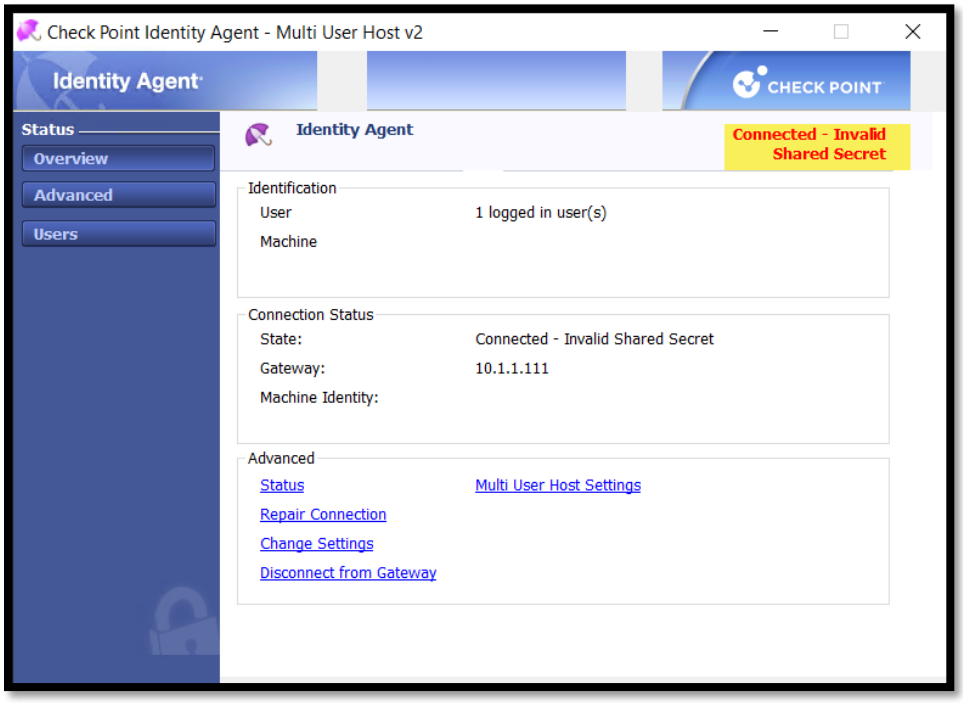
4. Copy the agent to the domain controller and install it. Configure it to connect to the GW over 10.1.1.111.



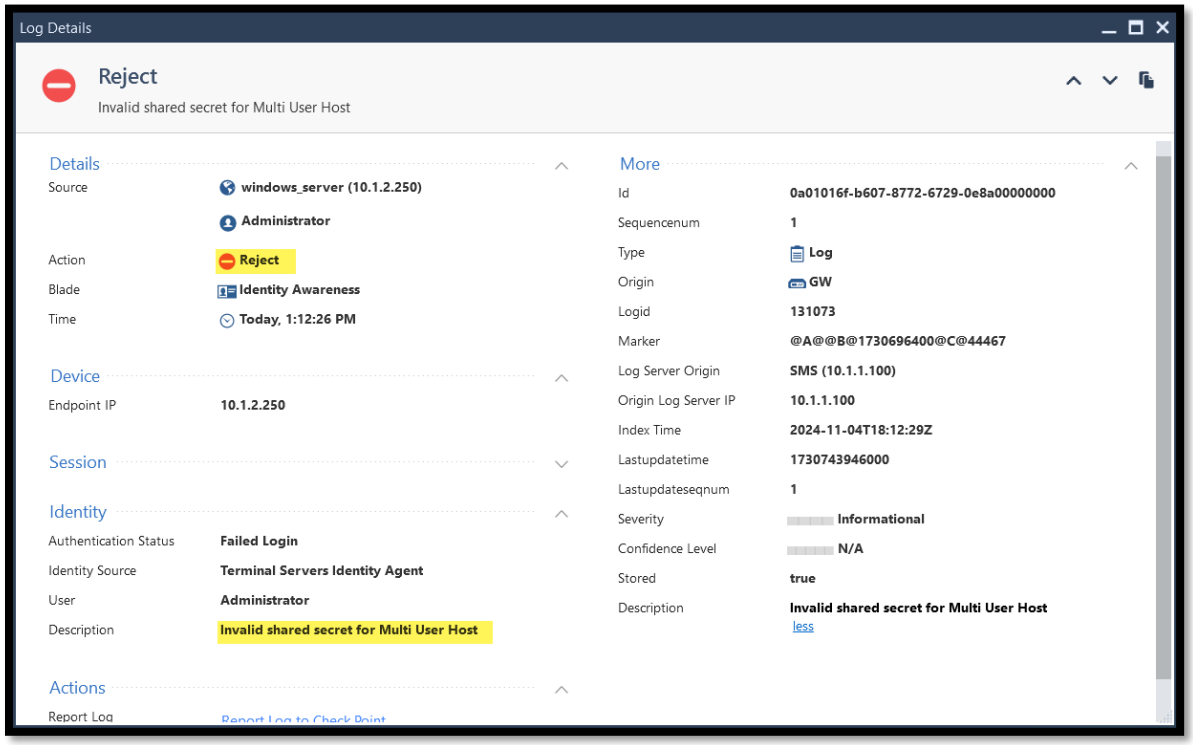
5. Try to connect this agent and trust the self-signed certificate.



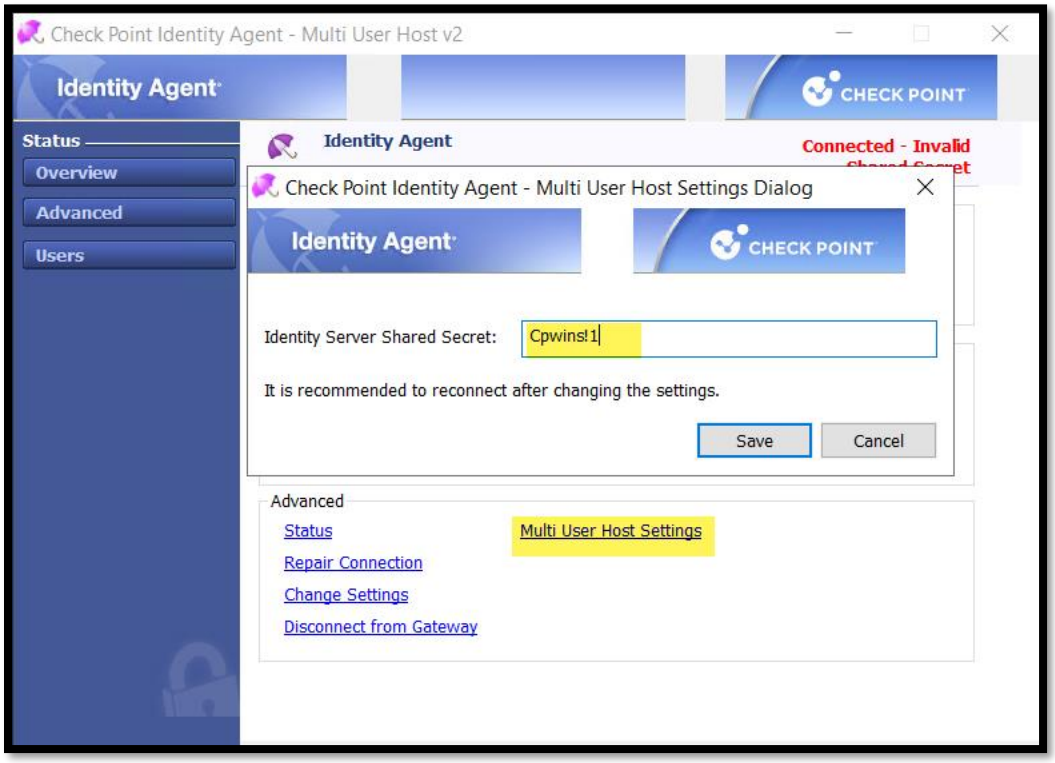
6. Notice that the connection will fail since we have not configured the Shared Secret in the agent yet.



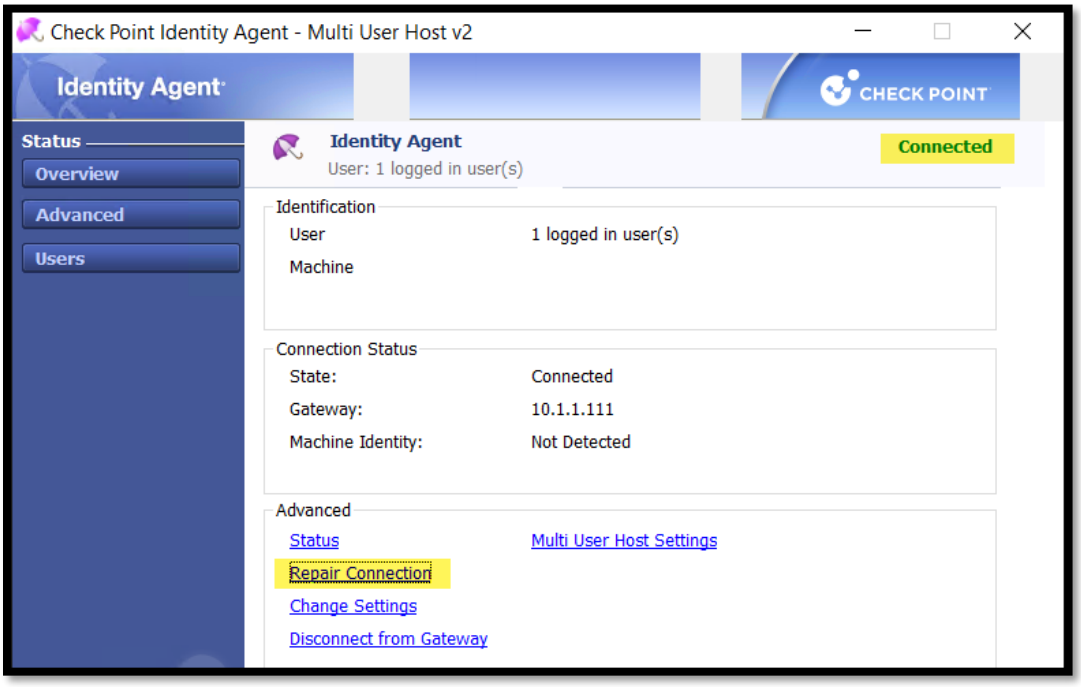
7. Review the Identity awareness logs and confirm you can see the related log.



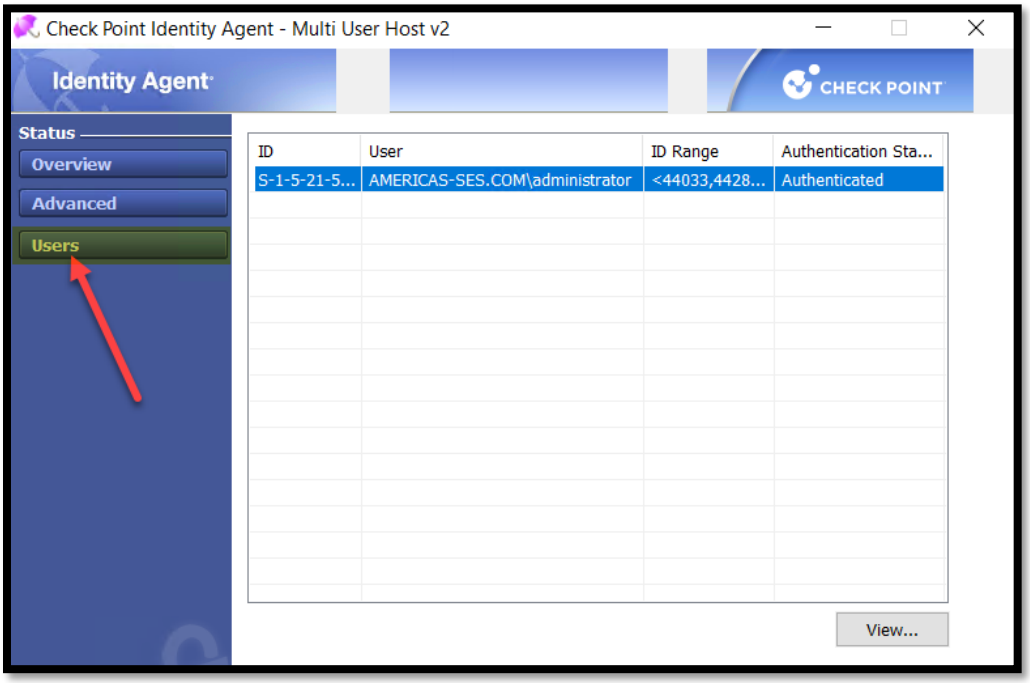
8. To enter the Shared Secret, click “Multi User Host Settings” and provide the secret we configured earlier and save the seetings.



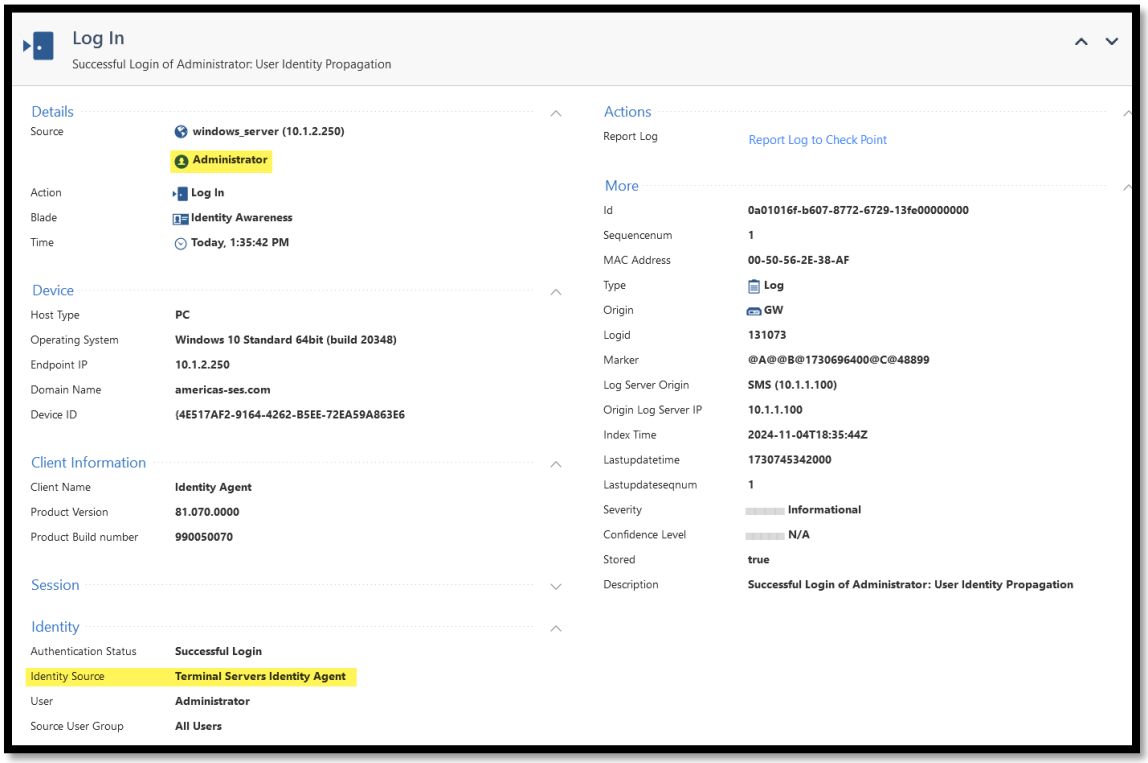
9. Try to connect again by repairing the connection and confirm the agent is now connected.



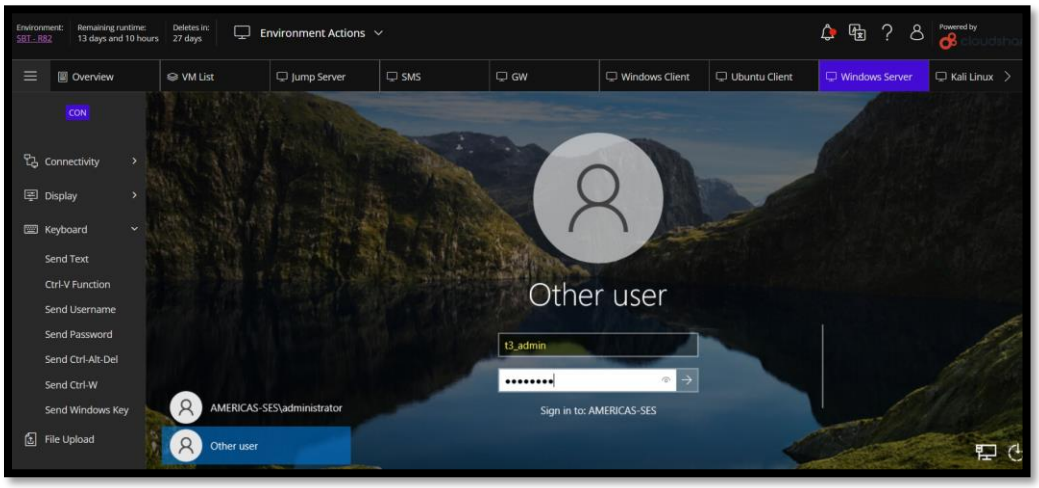
10. Under the users list in the agent, confirm you can see the current user in the list as an authenticated user



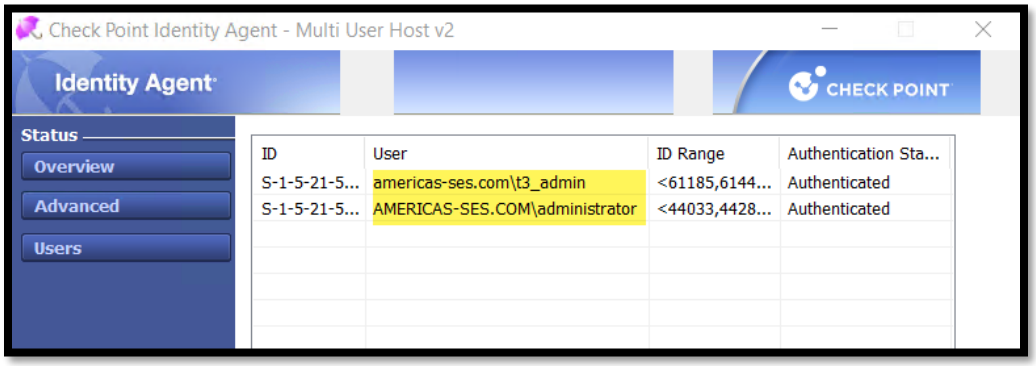
11. Review the logs and confirm the Administrator user was authenticated successfully.



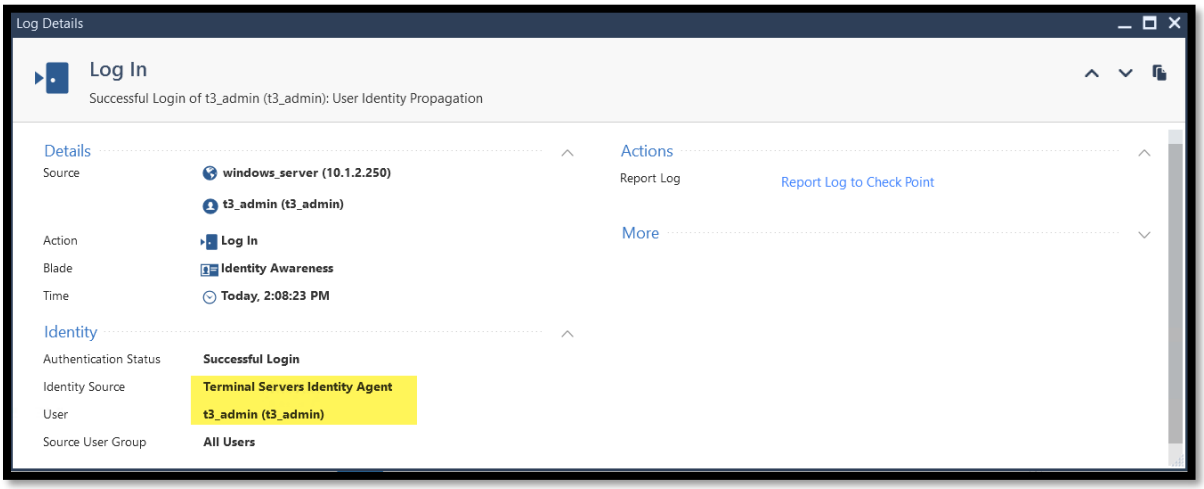
12. Return to the training environment and try to login with t3_admin/Cpwins!1 credentials.



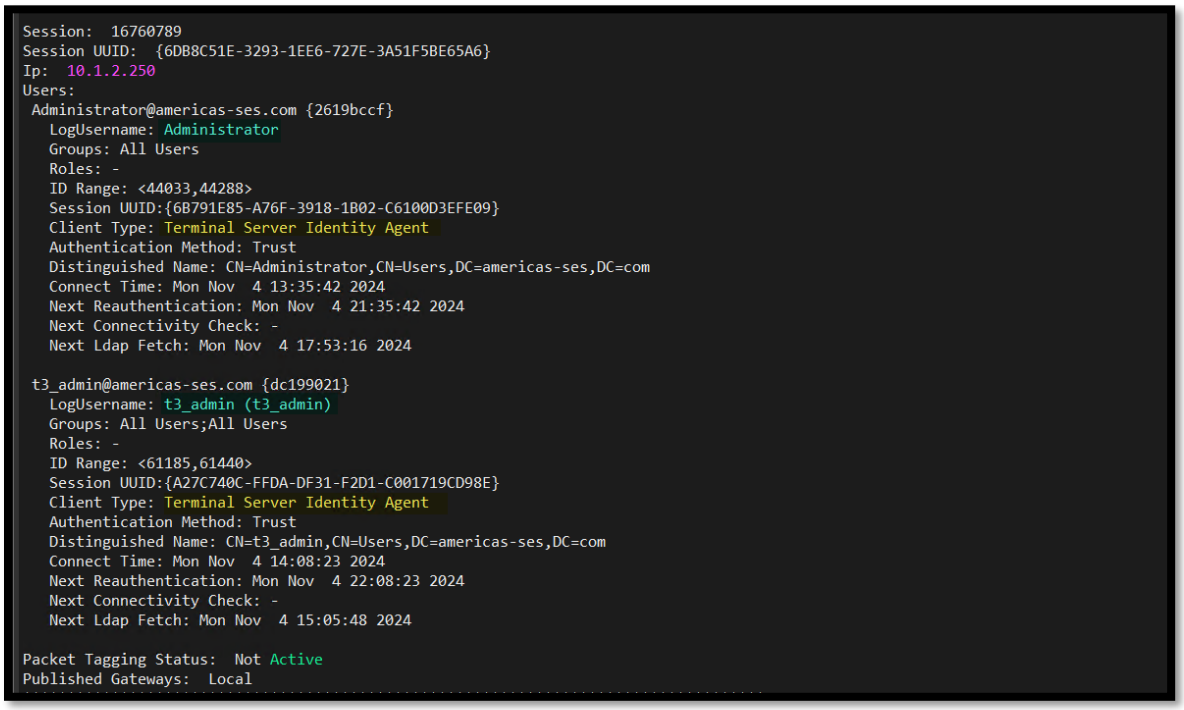
13. Return to the previous RDP connection and confirm that the new user is also identified



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



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

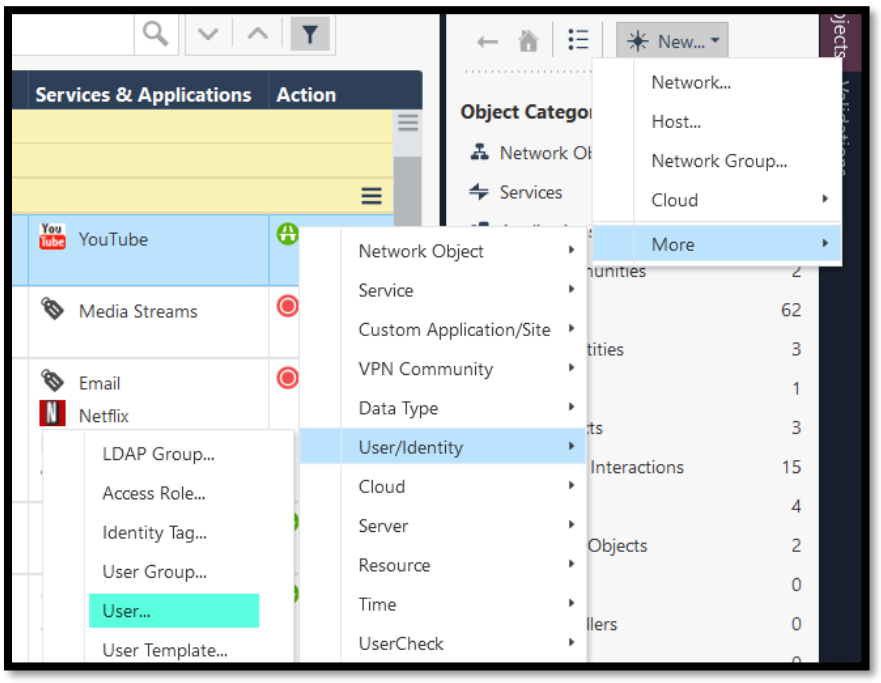


Exercise 5: Captive Portal

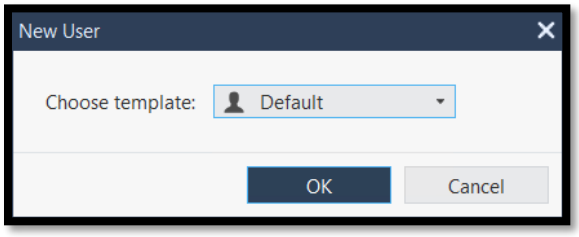
In the previous exercises, we configured various method of acquiring a user identity and use it for the security policy enforcement.

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.

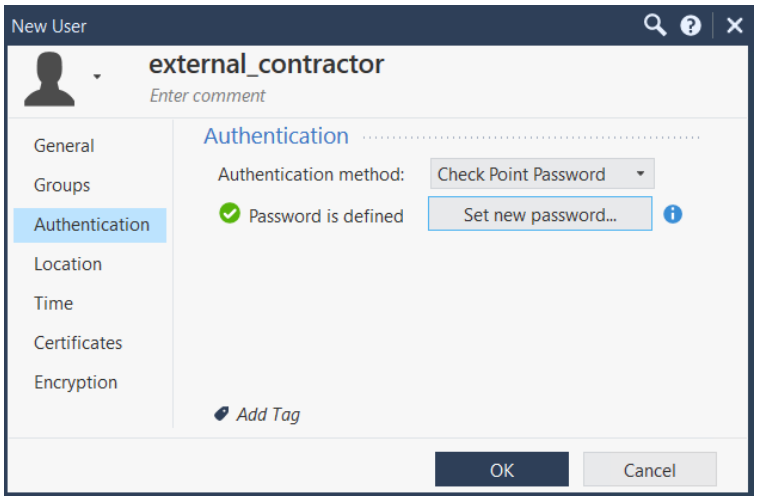
1. Create a new internal user in SmartConsole.
    a. New -> More -> User/Identity -> User



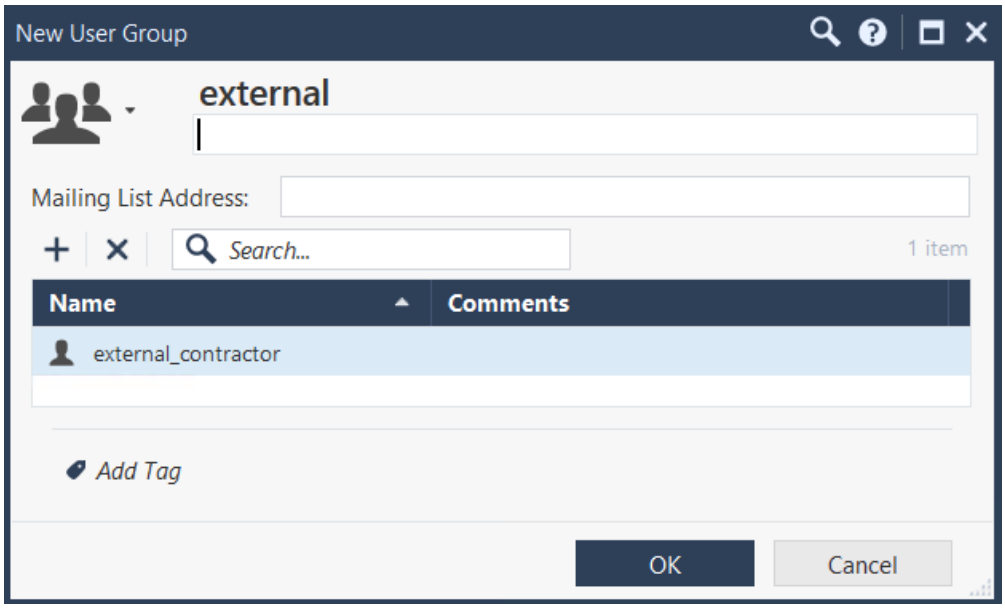
2. Select the default user template.



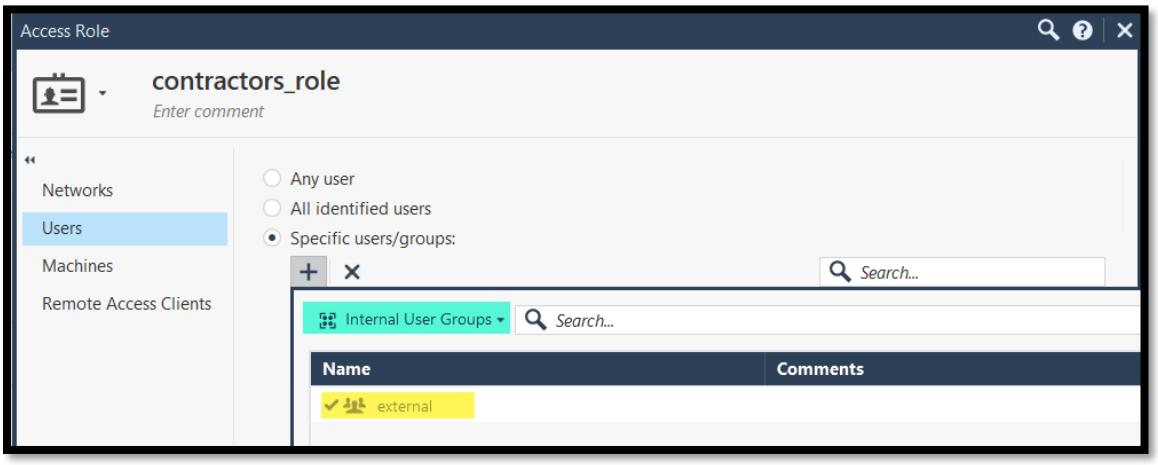
3. Give this user a name and configure the authentication as Check Point Password and set a proper password.



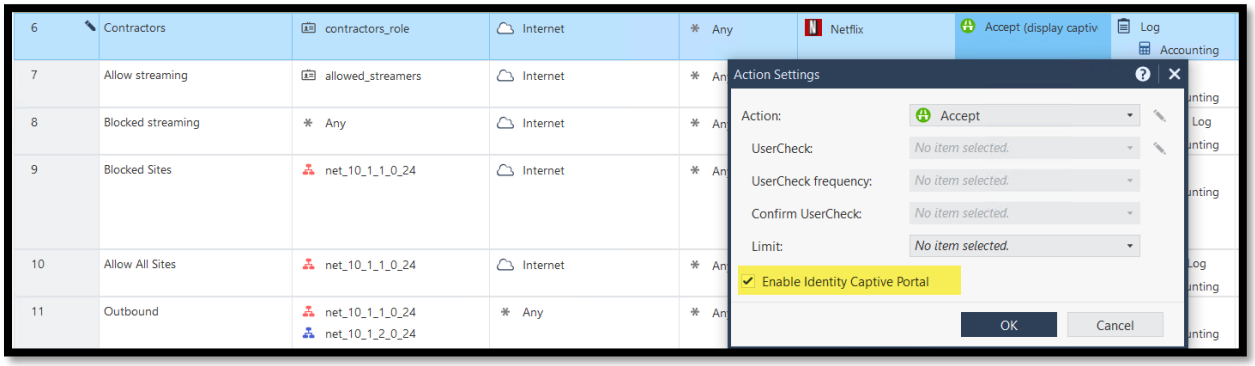
4. Add a new user group and add the user we created above to this group.
    a. New -> More -> User/Identity -> User Group



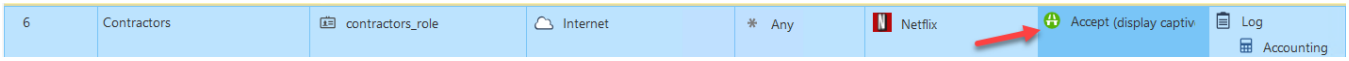
5. A Create a new Access Role and give it a proper name and add the new external User Group we created earlier.
    - Note that you need to change the default filter to be able to see Internal User Groups



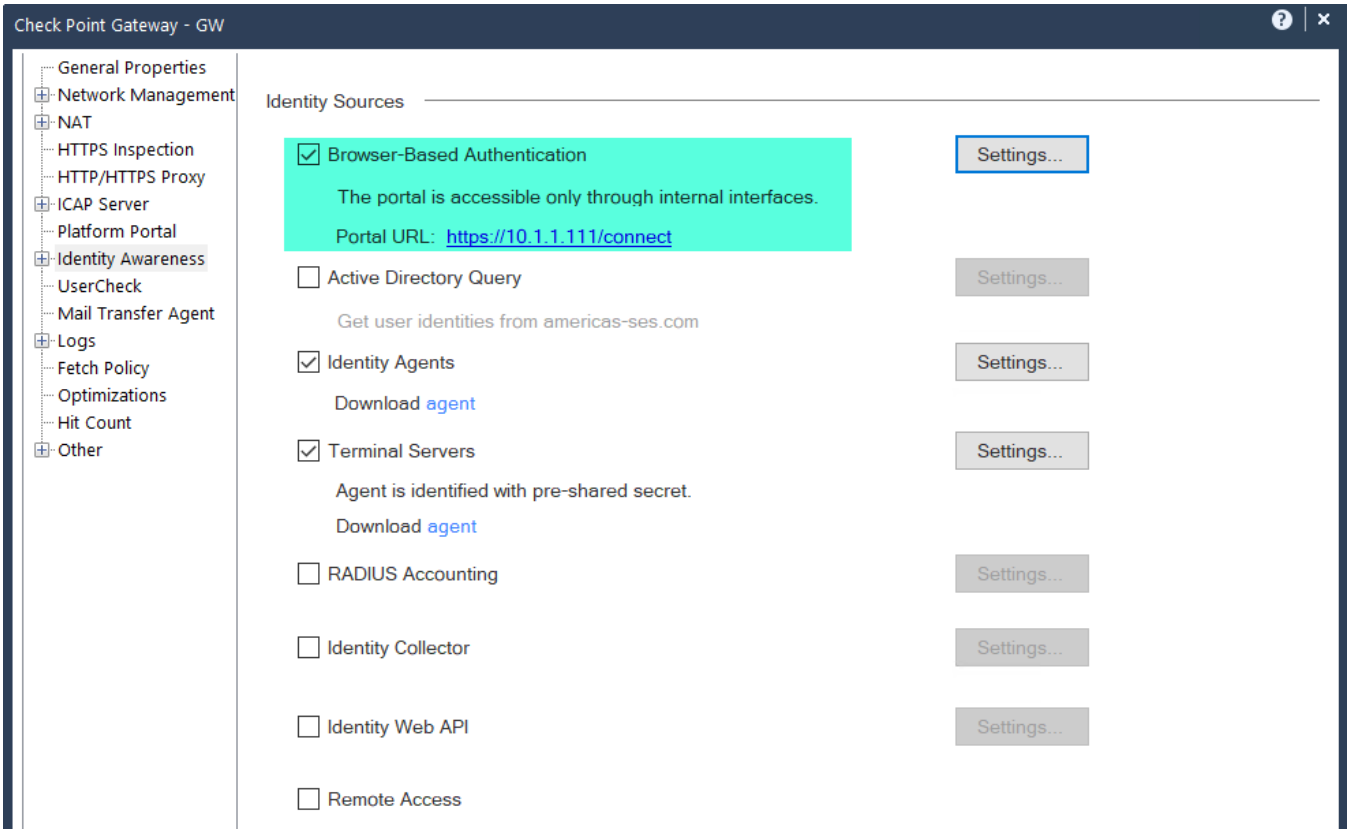
6. Create a new rule on top of the rule allowing YouTube. This rule will allow the contractors_role to access Netflix.
    - Note that we will need to modify the Action column to enable the Identity Captive Portal via More –> Action Settings. See below.



7. Confirm the final rule looks as expected.

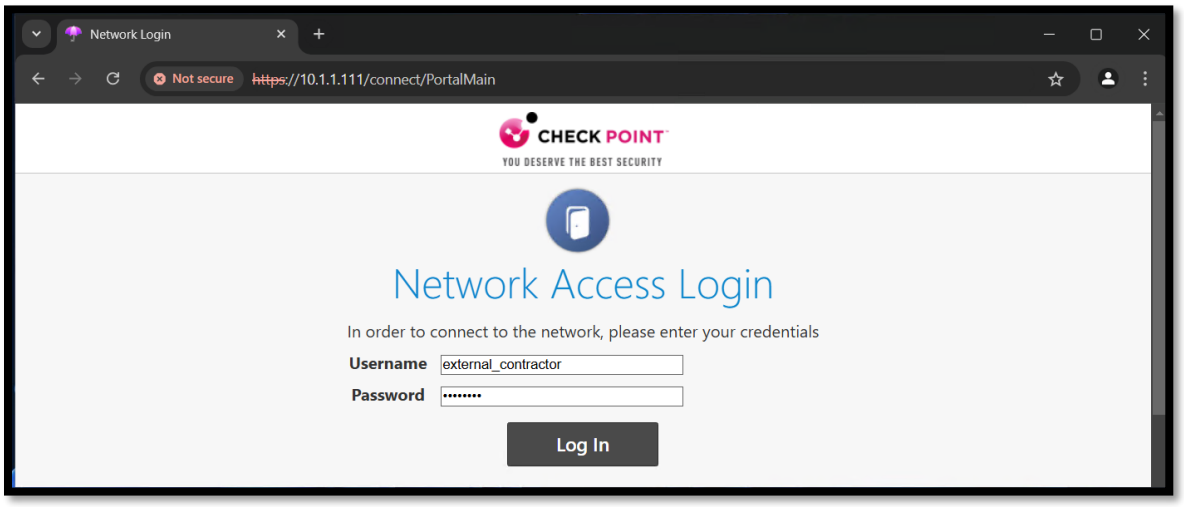


8. Edit the GW object and enable the browser-based Authentication

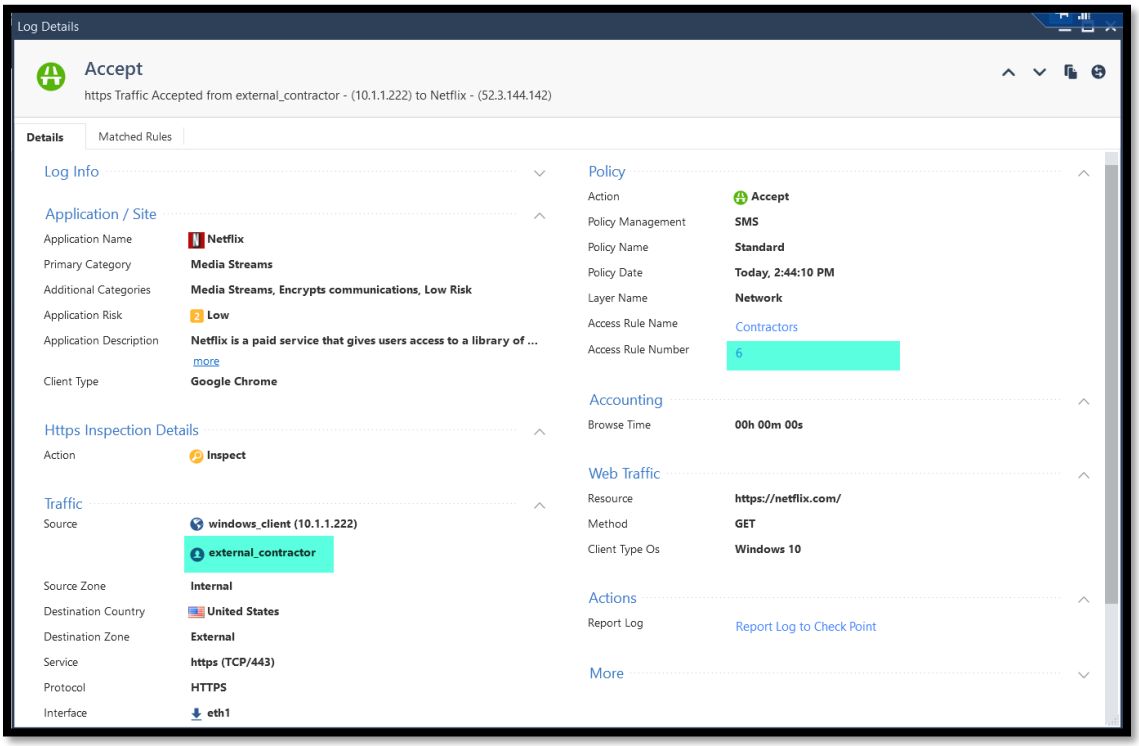


- Note that the external user is unknown to the GW. The user will be redirected to the Identity captive portal to provide the credentials.

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.



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.



End of Lab 3

