

Establishing Trust between Check Point Identity Collector and a Cisco ISE Server using self-signed certificates



Check Point Identity Collector

The Identity Collector gives a new, powerful, option to query for Active Directory events. The Identity Collector was designed specifically for heavy-load environments, with emphasis on Security Gateway performance.

The Identity Collector registers the AD Domain Controllers to receive login security events, parses those events and reports them to the Security Gateway.

Identity Collector Key Benefits over Standard AD Query

- Reduces the load on the Security Gateway - the Collector is doing the querying, parsing and caching instead of the Security Gateway
- Reduces the load on the DCs - the native Windows API used consumes less resources than the WMI protocol the gateway uses.
- AD user, which is used for fetching the events, requires no administrator or administrator-like permissions. Only event log reader group membership is needed.
- One agent can serve multiple gateways, even from different CMAs.

Cisco Identity Service Engine (ISE)

Cisco ISE provides a wealth of user identity, endpoint device, and network context information that is useful to many IT platforms for customers around the globe. To bring greater insight to risky user activities on the network, Cisco ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share identity, device, and network information. The IT infrastructure can serve more use cases and operate more effectively by becoming identity, device, and network aware. Cisco pxGrid is a unified framework that supports multivendor, cross-platform network system collaboration among IT infrastructures such as security monitoring and detection systems, network policy platforms, identity and access management platforms, and virtually any other IT operations platform.

Check Point and Cisco ISE Integration

The Check Point Identity Awareness Software Blade provides detailed visibility into users, groups, and machines. It provides application and access control through the creation of identity-based firewall policies in a Check Point deployment along with event monitoring and reporting. Cisco ISE integrates with Check Point's software blade to provide real-time and comprehensive identity and network privilege context. That includes user IP address, name, group, and Cisco TrustSec® security group tag information.

This integration provides Check Point gateways with better visibility of user activities while improving control of corporate resources. ISE helps the Check Point console to display contextual information associated with an event, such as the user's identity and level of access. This finer level of detail from ISE can reduce threats and data loss by restricting access to resources by users and devices.

Requirements:

Identity Collector on a Windows server meeting the following requirements:

- Windows Server 2008 R2, Windows Server 2012 or Windows Server 2012 R2.
- Has connectivity to the AD domain controllers of the organization using DNS, LDAP and DCOM
- It is also possible to install the Collector directly on one of the domain controllers.
 - If any Firewall software is installed on the Domain Controllers (including Windows Firewall), please make sure that the rules allow DNS, LDAP and DCOM traffic from the machine on which the Identity Collector is installed. With Windows Firewall, please allow the following rule: "Remote Event Log Management" --> "Remote Event Log Management (RPC)".
- Has connectivity to the gateway, over port 443
- Administrator account for Identity Collector installation

- Has .NET framework (version 4) installed on
- At least 4GB of RAM
- At least 10 GB free HD
- Microsoft Active Directory Server
- Microsoft DNS Services
- NTP Services on Active Directory Server
- Java JRE 1.8 or Higher
- Open SSL 64Bit
- Cisco ISE Appliance V2.1 or greater
- pxGrid context-exchange capabilities

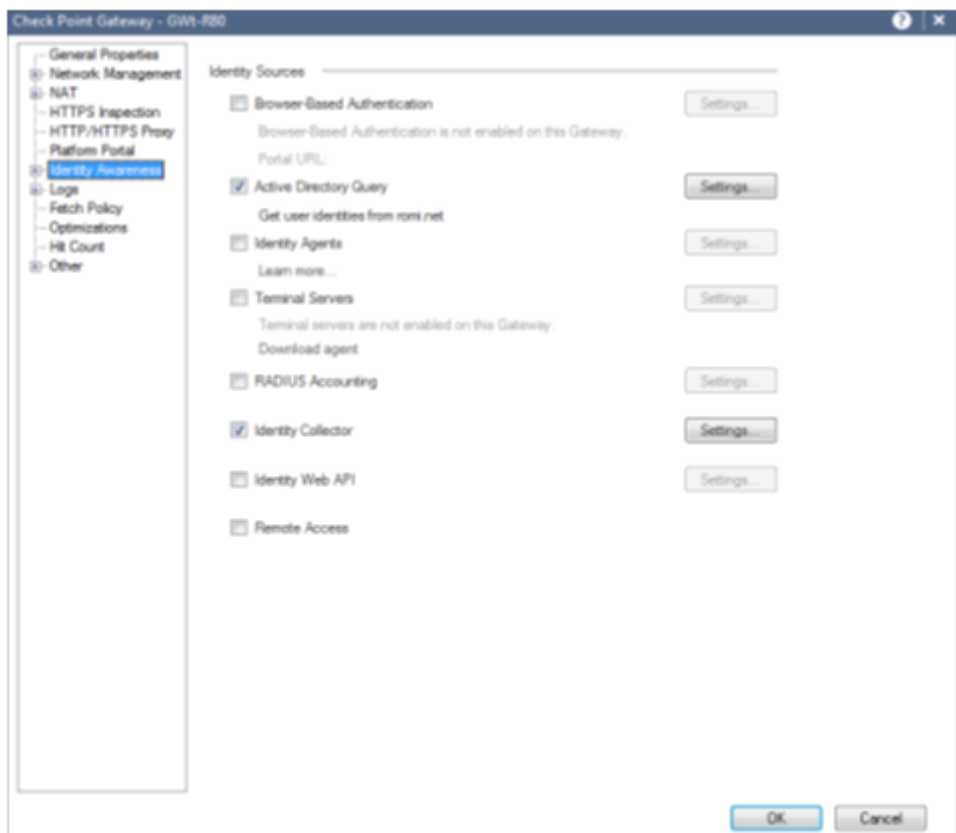
Additional requirements

- The Identity Collector requires an AD user that belongs to the default **Event Log Readers** group. No administrative role is required for this user.
- Install a hotfix on the Security Gateway (Available on top of R77.20 and R77.30)
- No AD schema changes are required.

Communication Protocols

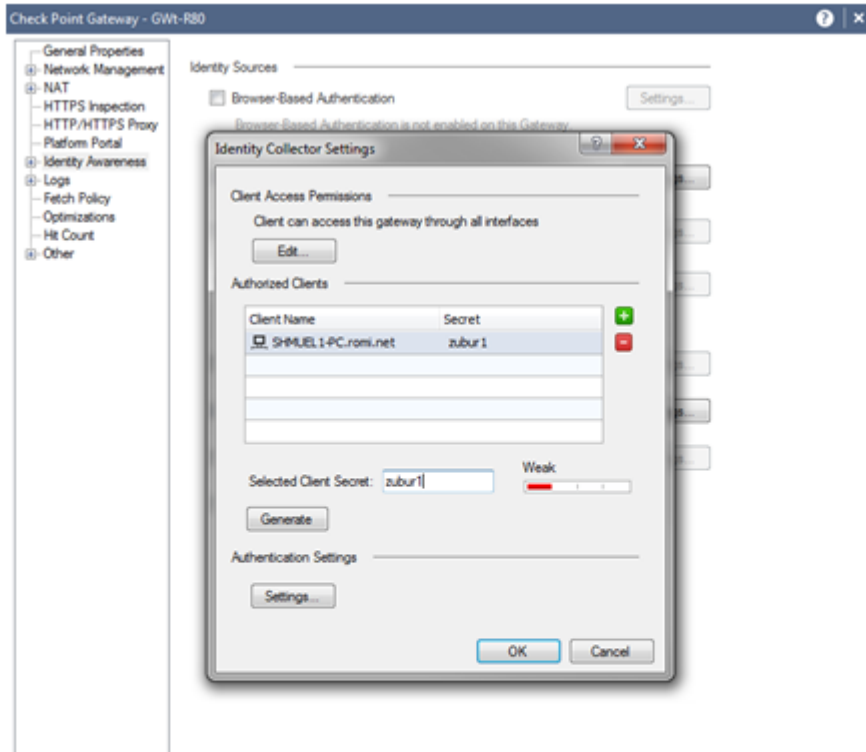
Direction	Port	Protocol
Identity Collector to gateway	443	Proprietary Check Point protocol, over HTTPS. Used for ongoing communication between the agent and the gateway
Gateway to Domain Controller	389/636	LDAP/LDAP over SSL
Identity Collector to Domain Controller	53	DNS
Identity Collector to Domain Controller	389	LDAP
Identity Collector to Domain Controller	135, and dynamically allocated ports	DCOM protocol, which makes extensive use of DCE/RPC.

Configuring the Security Gateway

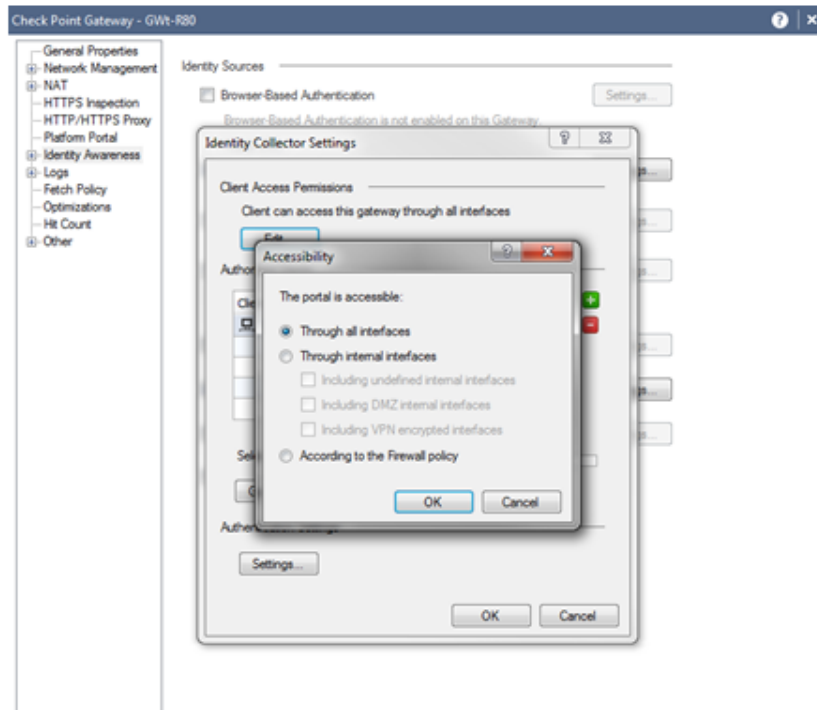


After enabling Identity Awareness enable Identity Collector and press Settings button

Note: Make sure to uncheck Active Directory Query



Create an Host with the Name and IP of the Identity Collector machine and add this host to the Authorized Clients.
Choose the Selected Client Secret.
Press on Edit



- Choose Through all interface
- Press OK until all being configured
- Install policy

Note: In some cases you may have to run from the gateway command line

- `pdp idc enable`

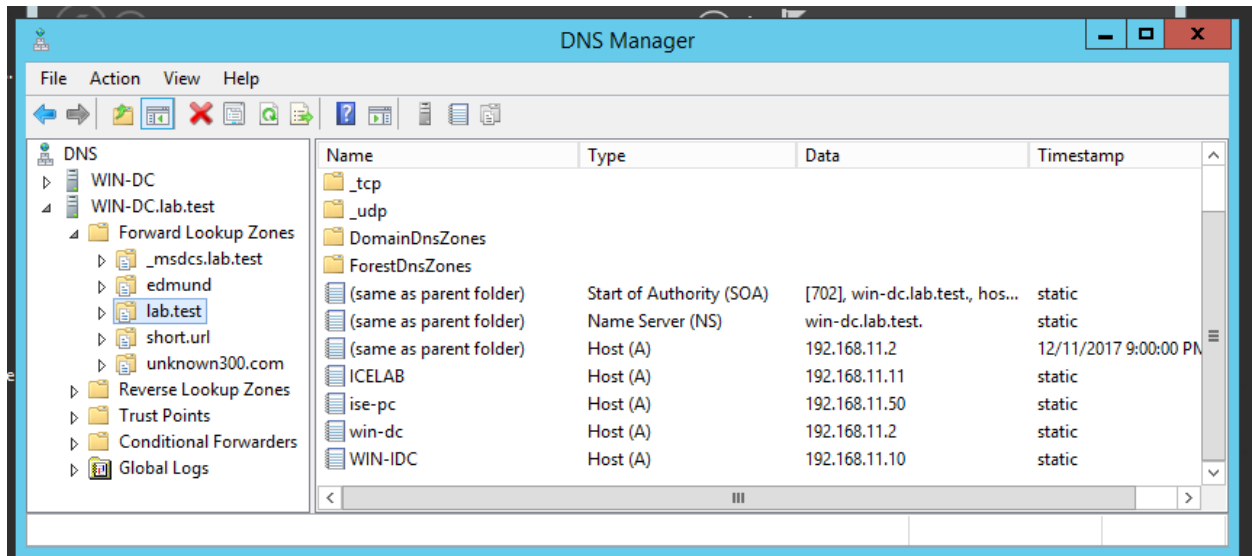
Configuring Identity Collector on Windows Server

Before moving forward make sure of the following

- Create a firewall rule allowing communication between the IDC and the Gateway

No.	Name	Source	Destination	VPN	Services & Applications	Content	Ac
1	Management	WIN_Victim Identity-Collector ED-VMInterface ED-VMInterface-172	R80-10	* Any	https ssh_version_2	* Any	

- Download the IDC software to the Windows Server from :
 - a. https://<IP_of_Security_Gateway>/_IA_IDC/download/CPIIdentityCollector.msi
- Verify DNS is running on the Domain Controller
- Verify the time is correct on the DC and ISE appliance
- Verify the DC/IDC or another server is setup as an NTP server
- Verify an A-Record exist for the ISE appliance



Adding New Domain

Identity Sources

Status	Type	Name	Host	Domain Name	Site Name	Total Events Reviewed	Events In Last Hour	Events In Last Minute	Last Event Sent Time	Status Description	Comment
OK	Active Directory	shk4k2052-172-gli-ids	172.23.57.173	gli-ids	shk4k2052-172-gli-ids	46	46	3	11:05:39	Success	

Source Info

Host Name shk4k2052-172-gli-ids	Status Connected	Total Events Sent 46	Domain Name gli-ids
Comment	Status Description Success	Events In Last Hour 46	In Events Collector False
IP Address 172.23.57.173	Type Active Directory	Events In Last Minute 3	
Site Name shk4k2052-172-gli-ids		Last Event Sent Time 11:05:39	

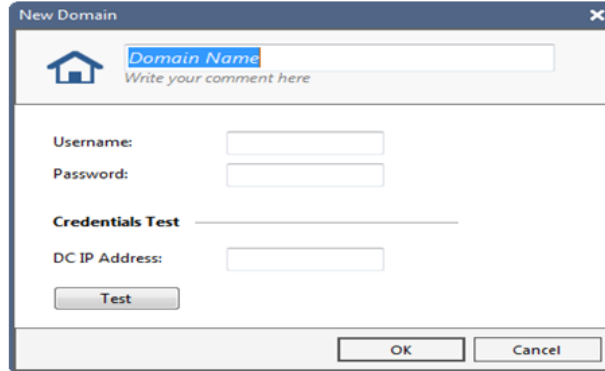
Press on Domains Icon

Domains

Name	Comment
------	---------

OK

Press on New Icon



1. Fill all the details:

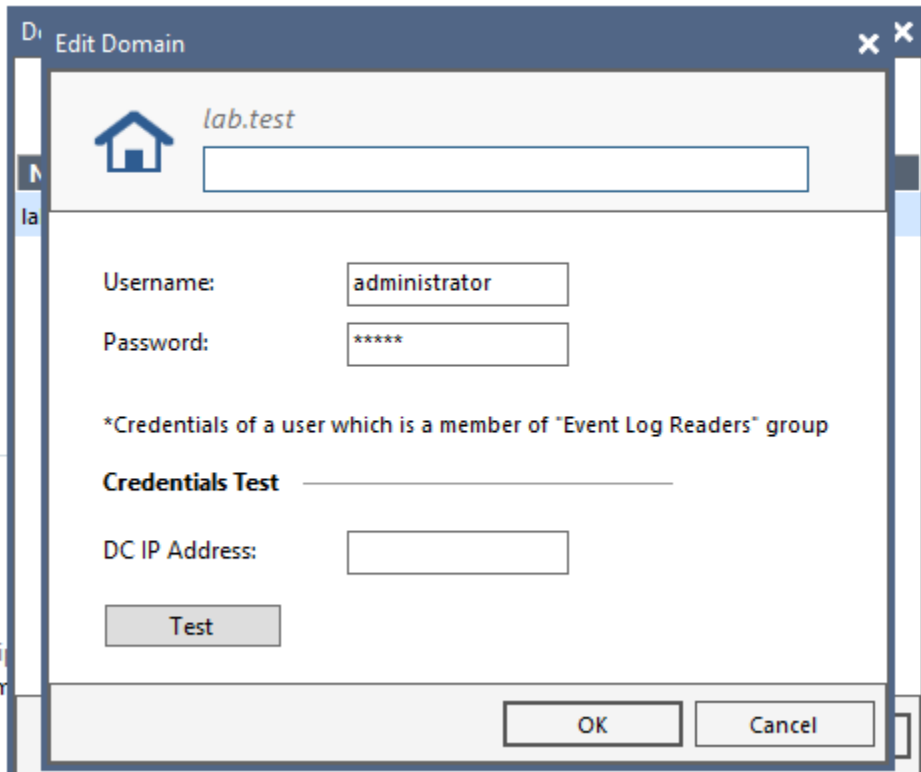
Domain Name- The real domain name

Comment- Add comment regarding the domain or leave empty

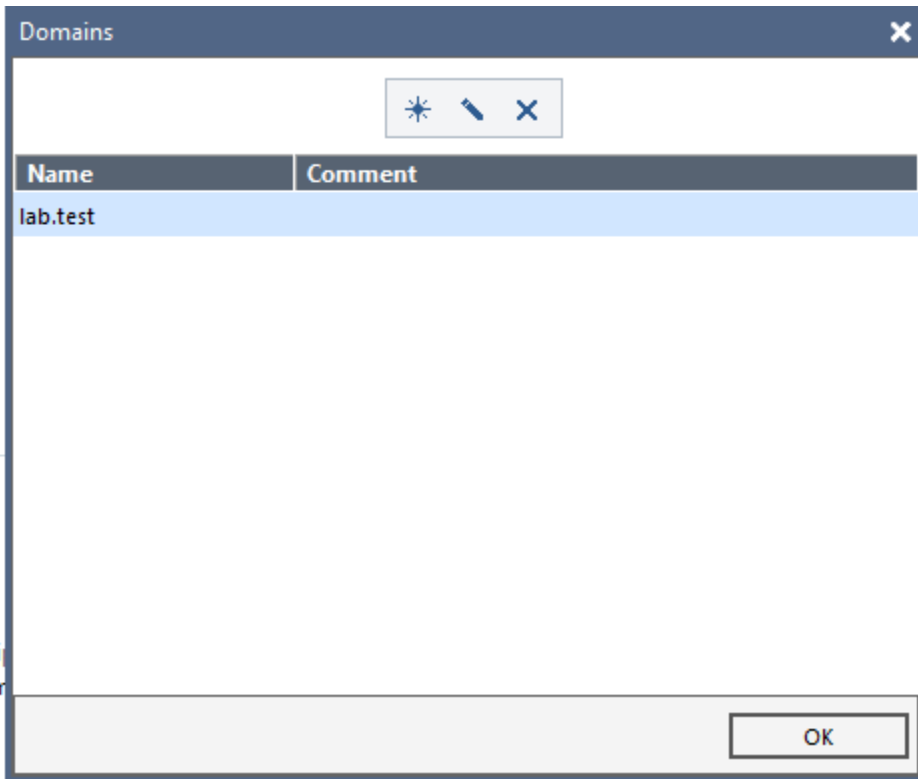
Credentials- Username and password are for all the DCs in this Domain

DC IP Address- In order to check the credentials fill one of the DCs' ip and press Test button

2. Press OK

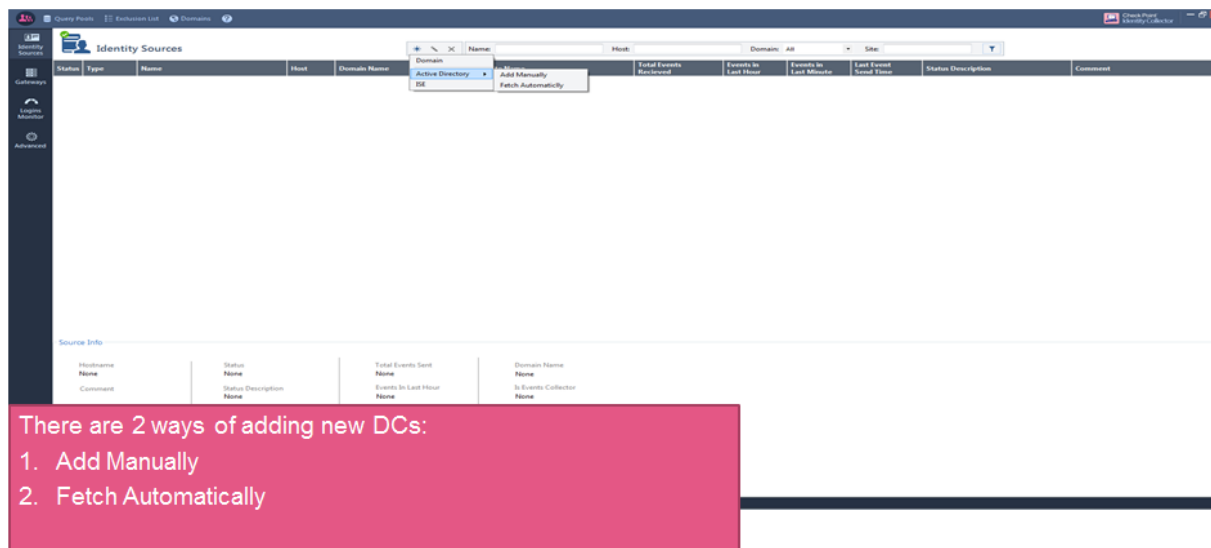
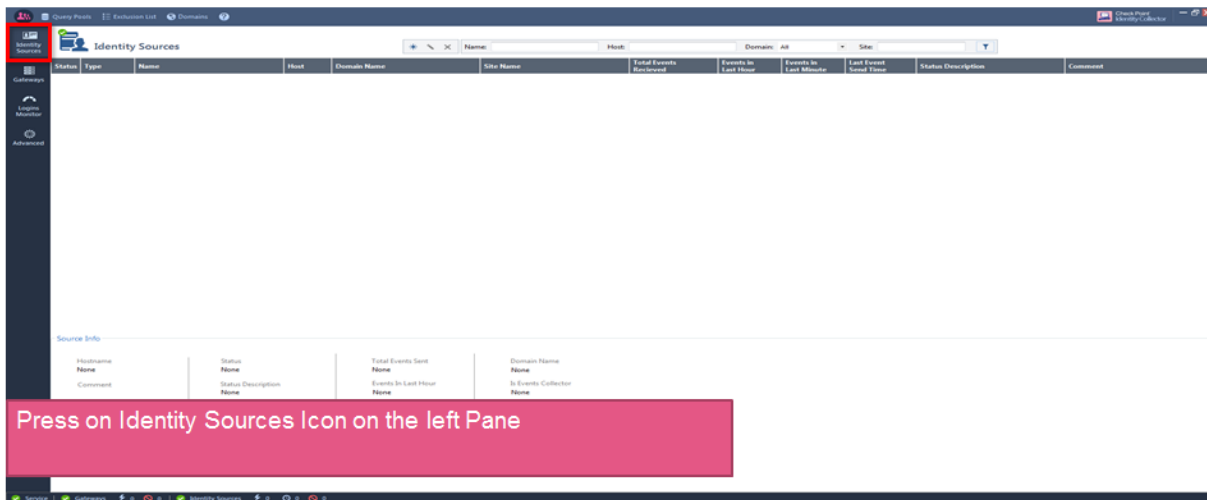


Test Credentials succeeded

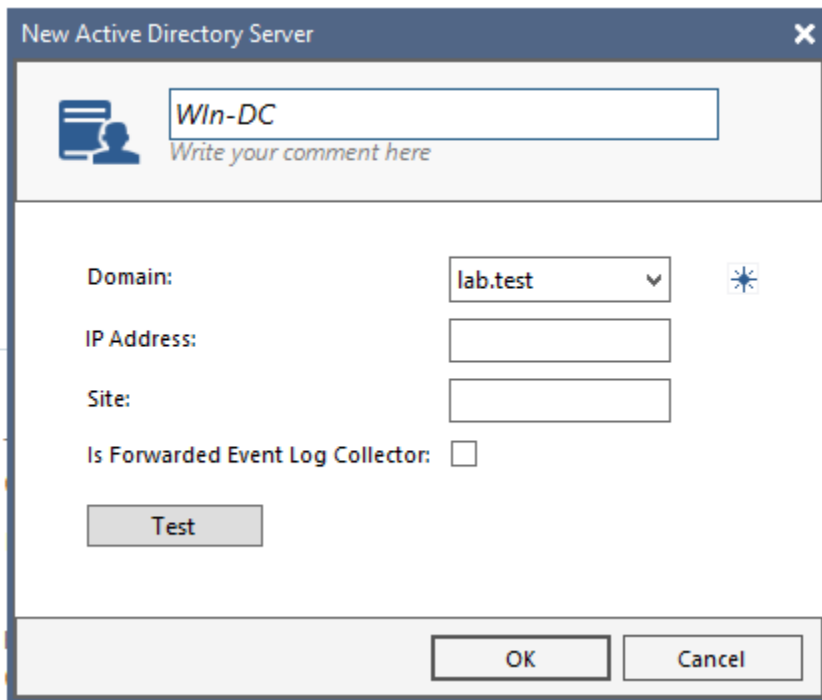


- The domain was added
- Press OK button

Adding New Domain Controllers



Adding new DCs- Add Manually



New Active Directory Server

Win-DC
Write your comment here

Domain: lab.test

IP Address:

Site:

Is Forwarded Event Log Collector:

Test

OK Cancel

Fill all the details:

Domain-Choose one of the domains configured in the previous phase

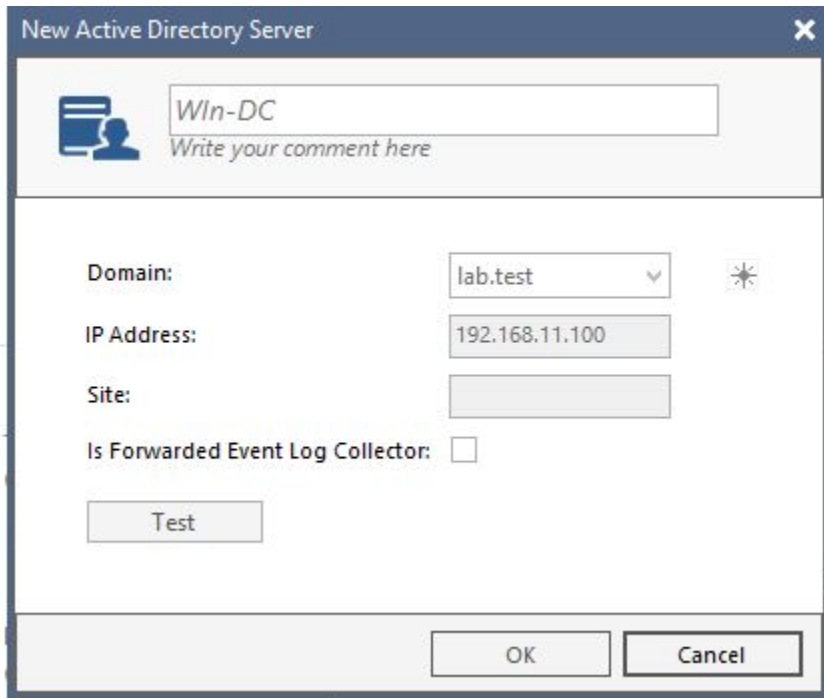
Domain Controller Name- Name of the DC

Comment-Add a comment

IP Address of DC-The Identity Collector will subscribe to this IP

Site- The site that the DC is in (Optional)

Event Log Collector- in case this checkbox is checked the identity collector will read the events from the forwarded events (this is usually disables)



2. Test Connectivity- you might want to check the connectivity to this DC
3. Press OK

Adding new DC- Fetch Automatically

Domain: lab.test

DC IP Address: 192.168.11.100

Fetch

Fetched Servers

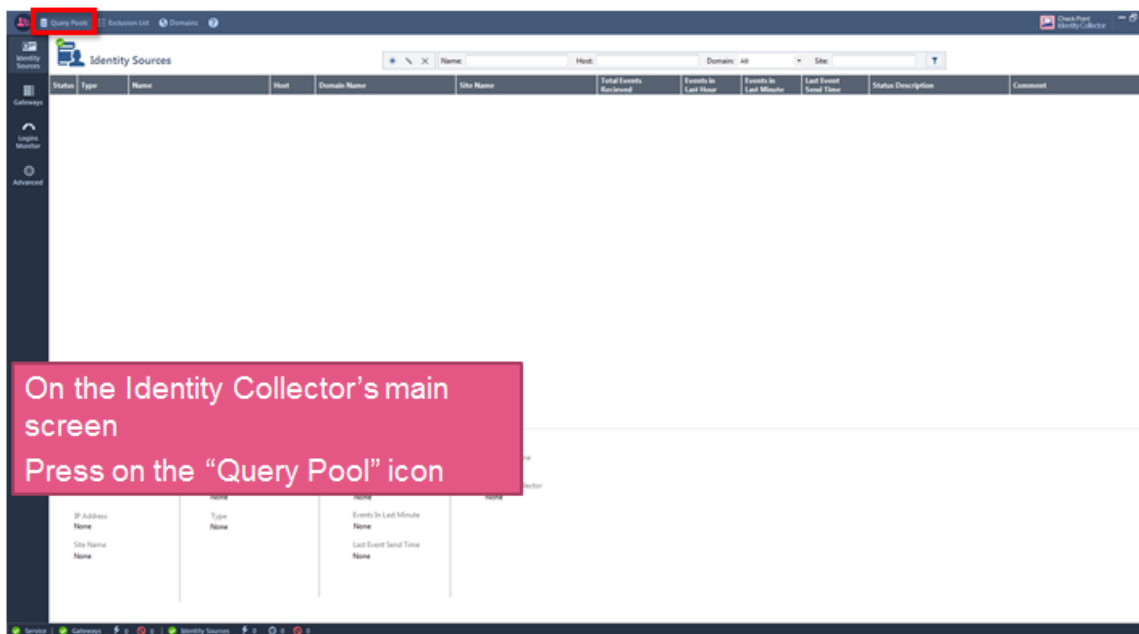
Enabled	Name	Address
---------	------	---------

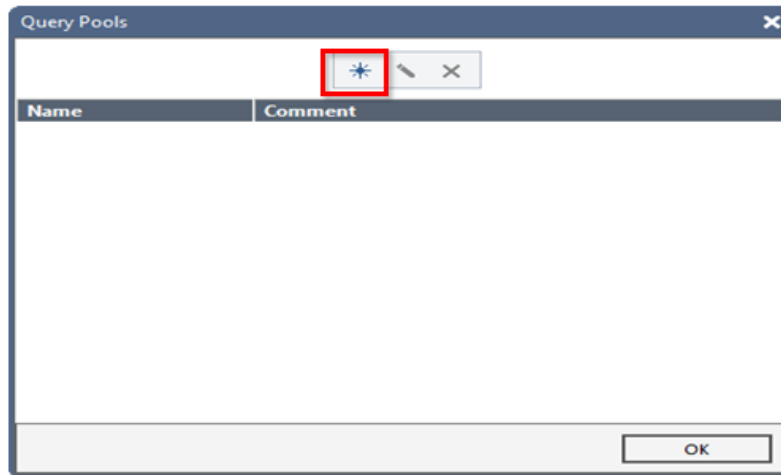
OK Cancel

3. Choose the DCs you want to add. Please notice that if one DC has more than 1 interface, it will appear once for every interface. It is highly recommended to choose only one interface.
4. Press OK

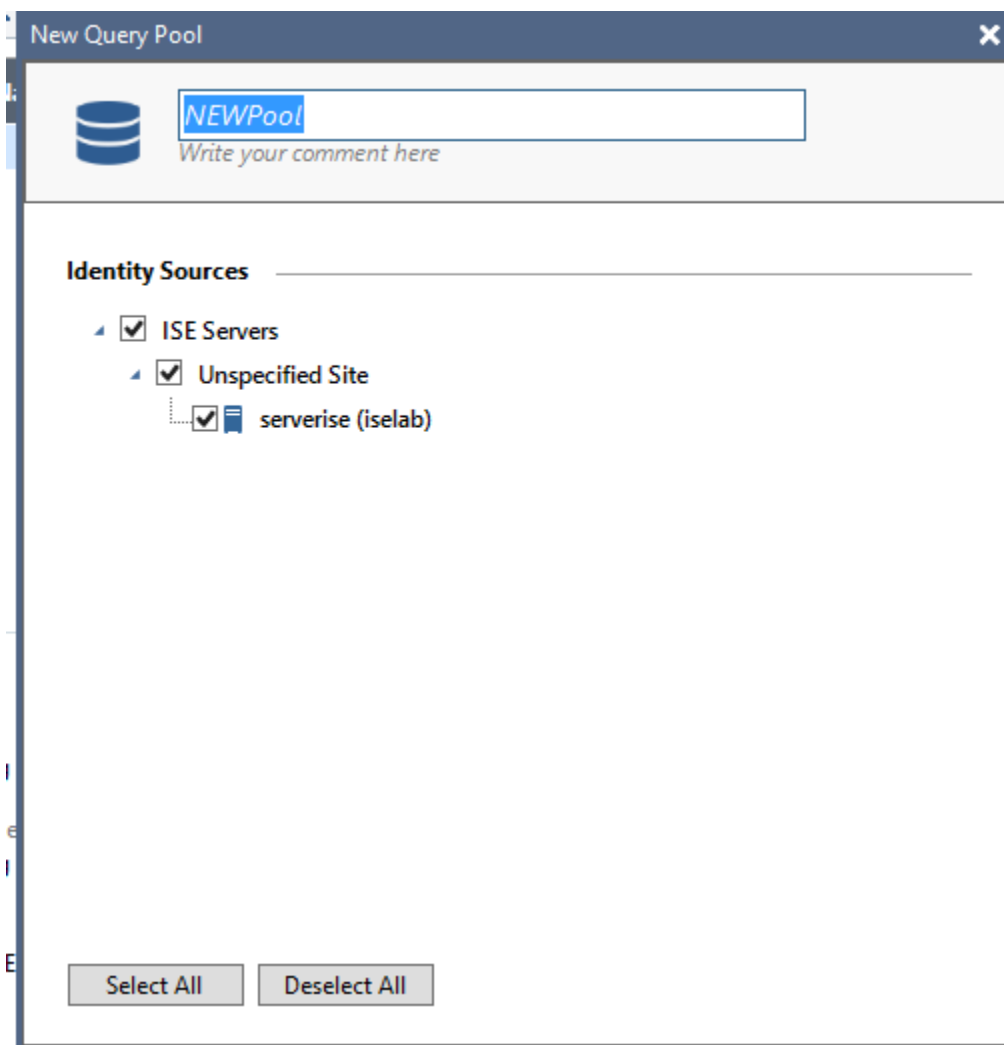
Adding New Query Pool

- Query pool is an object that collects few DC's together. The Security Gateway configuration specify a query pool, meaning only events from those DC's will be sent to the Security Gateway
- You may create several Query Pools with different combinations
- Events **won't be sent** to the Security Gateway unless a Query Pool is chosen for it





- No query pools exist yet
- Press New icon



1. Select the DCs to query from
2. Give a name to the query pool
3. Press OK

Adding Security Gateway

Press on Gateways icon on the left pane

Press on new icon

New Gateway

Object Name: gw
Write your comment here

Server Info

IP Address:

Shared Secret:

Query Pool: queryExample

Pre R80.X Gateway:

Test

Certificate Info

Fingerprint: unresolved
Name: unresolved

OK Cancel

- Fill the name, ip and shared secret of the Security Gateway
- Choose a query pool
- Press on Test
- Notice: In case of cluster, enter the cluster IP and not the member's IP

New Gateway

gw
Write your comment here

Server Info

IP Address: 172.23.57.172

Shared Secret: *****

Query Pool: queryExample

Pre R80.X Gateway:

Test Untrusted certificate - Please Initiate Trust

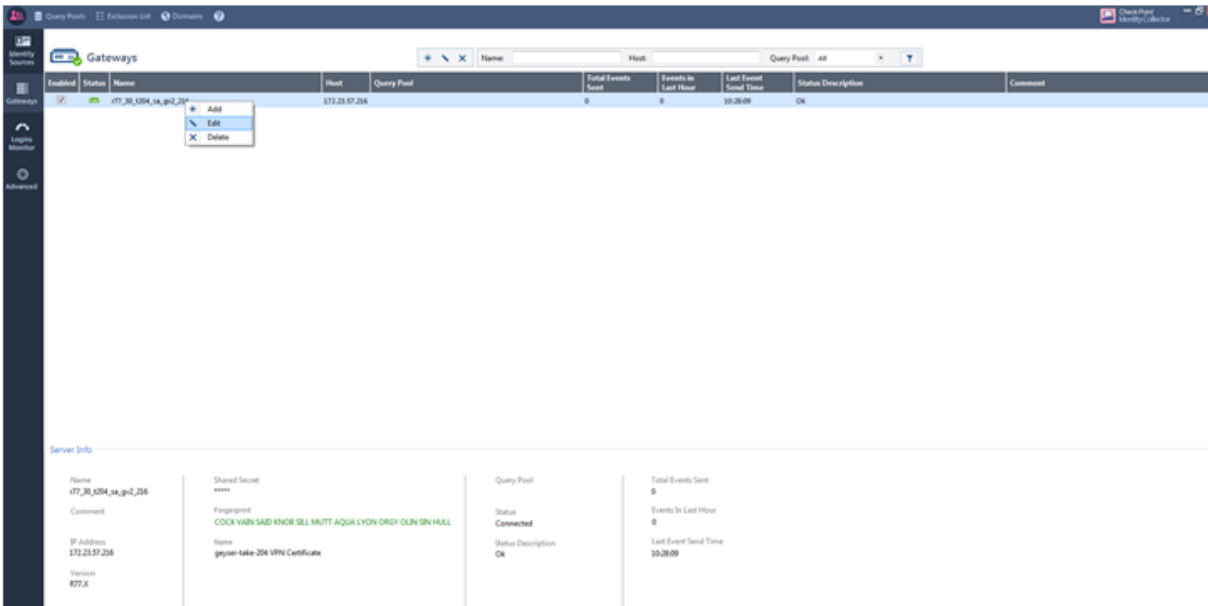
Certificate Info

Fingerprint: NOB SUP TIC SPY LISA ULAN LAUD OAT RUB BUN GLOW SLUG
Name: zivkstd172 VPN Certificate

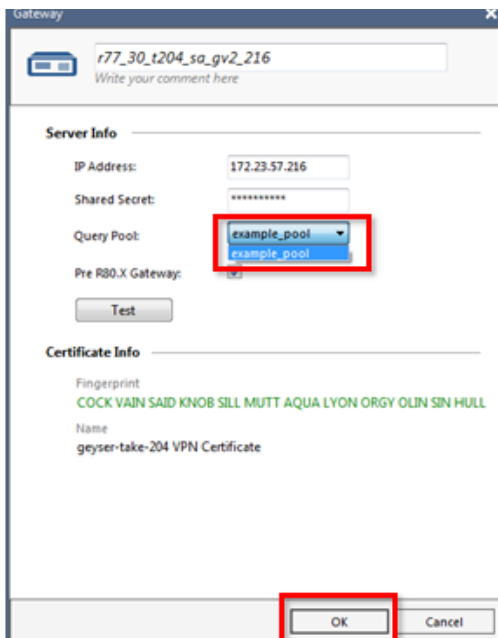
Trust

OK Cancel

Check the fingerprints.
Press on Trust



1. Go to "Gateways" on the left pane
2. Right-click the Security Gateway
3. Click "Edit"

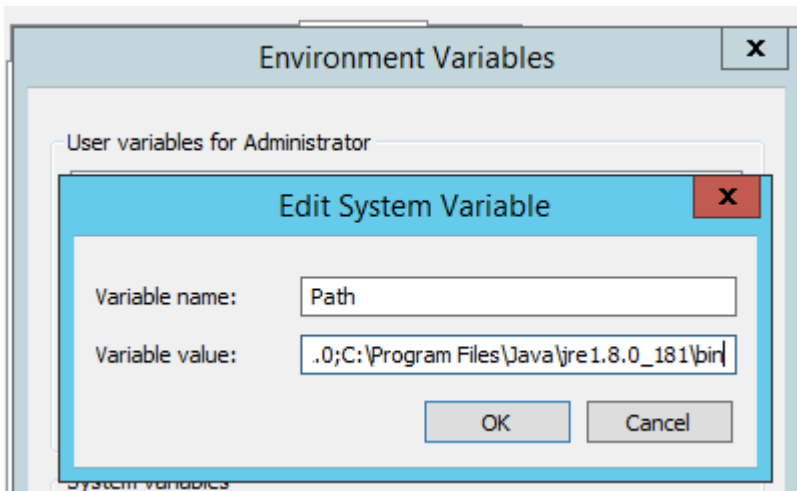


1. Choose the desired Query Pool
2. Press "Ok"

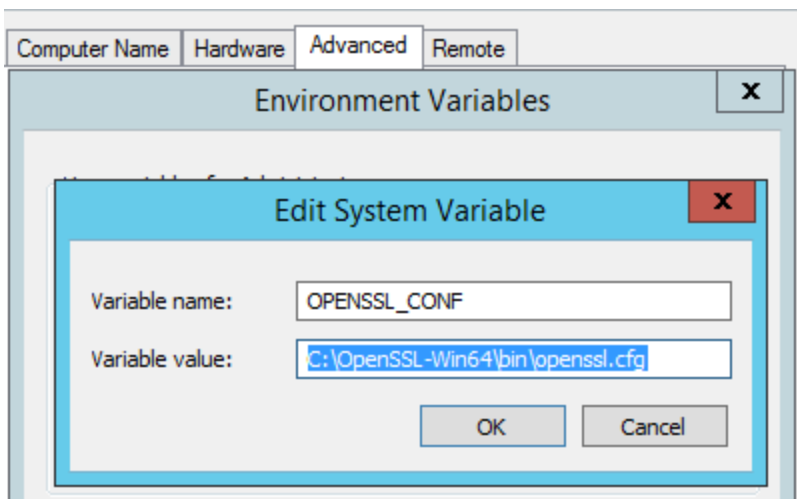
Procedure to Create JKS Certificates and Establish Trust

Before continuing make sure of the following

- Install Java 1.8 or higher(can be on the same Windows used for IDC)
- Make sure you have added java to your Environment Path (needed for KeyTool)



- Install OpenSSL 64bit and add to Environment Path



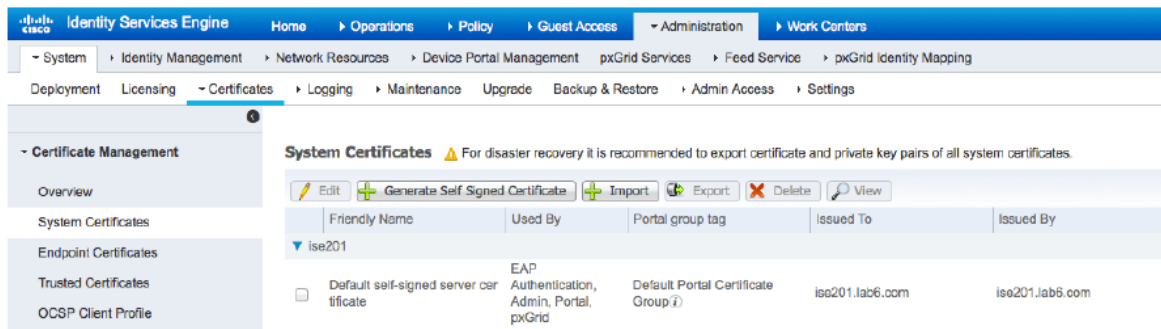
- Very connectivity to the Cisco ISE Server WebUI

Make sure your AD domain is up and running before you configure ISE. The ISE setup configuration will require the host name, IP address, domain name, DNS and NTP server names.

ISE, pxGrid client, and PC client must be FQDN resolvable.

ISE pxGrid Setup

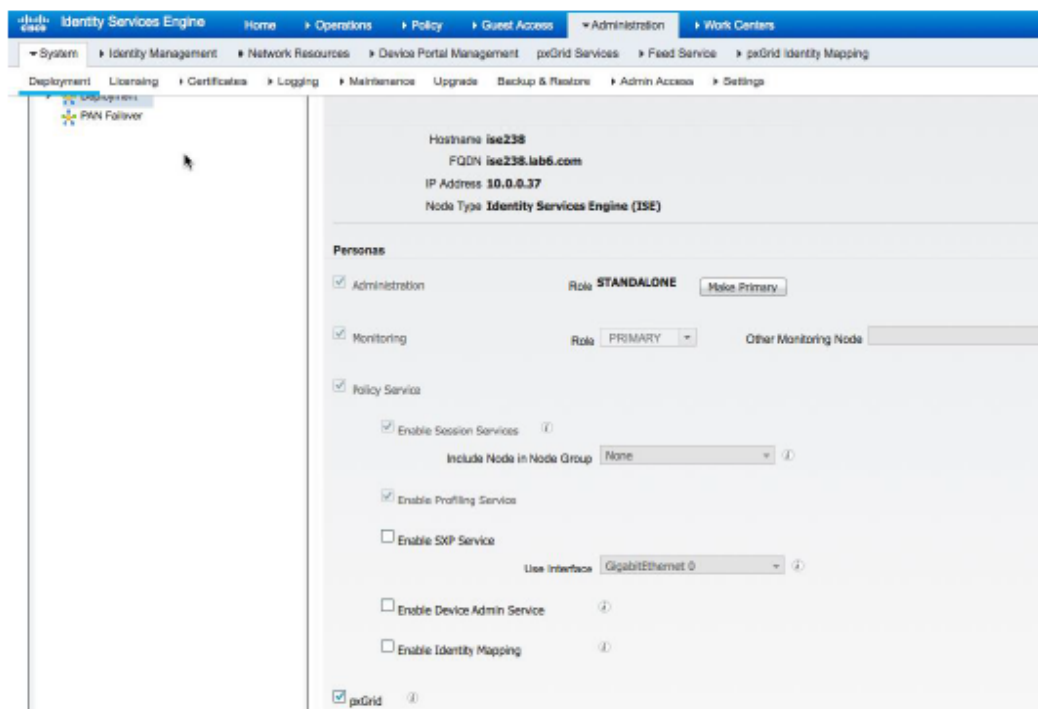
Step 1 Select **Administration->Certificates->** note the default self-signed certificate



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The left sidebar shows the navigation menu with 'Certificates' selected. The main content area is titled 'System Certificates' and includes a warning: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below this, there are buttons for 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. A table lists the certificates:

Friendly Name	Used By	Portal group tag	Issued To	Issued By
ise201				
<input type="checkbox"/> Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	ise201.lab6.com	ise201.lab6.com

Step 2 Enable pxGrid persona
Select **Administration->System Deployment->Enable pxGrid node**



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The left sidebar shows the navigation menu with 'System Deployment' selected. The main content area displays the configuration for the 'ise238' node. The node details are: Hostname: ise238, FQDN: ise238.lab6.com, IP Address: 10.0.0.37, Node Type: Identity Services Engine (ISE). The 'Personas' section is expanded, showing the following configuration:

- Administration: Role STANDALONE, Make Primary button
- Monitoring: Role PRIMARY, Other Monitoring Node: [Empty field]
- Policy Service
 - Enable Session Services: Include Node in Node Group: None
 - Enable Profiling Service
 - Enable SXP Service: Use Interface: GigabitEthernet 0
 - Enable Device Admin Service
 - Enable Identity Mapping
- pxGrid

Step 3 You should see ISE published topics of information from the MNT node

Note: This may take a few minutes to come up

The screenshot shows the Cisco Identity Services Engine Administration console. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and pxGrid Identity Mapping. The 'Clients' tab is active, showing a table of clients. The client 'ise-mnt-ise238' is selected, and its 'Capability Detail' is expanded. The table below shows the following data:

Capability Name	Capability Version	Messaging Role	Message Filter
Core	1.0	Sub	
IdentityGroup	1.0	Pub	
SessionDirectory	1.0	Pub	

Step 4 You should see ISE published topics of information from the Admin node

The screenshot shows the Cisco Identity Services Engine Administration console. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and pxGrid Identity Mapping. The 'Clients' tab is active, showing a table of clients. The client 'ise-admin-ise238' is selected, and its 'Capability Detail' is expanded. The table below shows the following data:

Capability Name	Capability Version	Messaging Role	Message Filter
GridControllerAdminService	1.0	Sub	
AdaptiveNetworkControl	1.0	Pub	
Core	1.0	Sub	
EndpointProfileMetaData	1.0	Pub	
EndpointProtectionService	1.0	Pub	
TrustSecMetaData	1.0	Pub	

Certificate Procedure

1. Generate the private key:

```
openssl genrsa -out alpha.key 4096
```

2. Generate the self-signed CSR (e.g., alpha.csr) request and provide a challenge password:

```
openssl req -new -key alpha.key -out alpha.csr
```

Note: You can leave everything blank besides the "challenge password".

3. Generate self-signed cert public-key pair certificate:

```
openssl req -x509 -days 365 -key alpha.key -in alpha.csr -out alpha.cer
```

4. Generate PKCS12 file (.p12) using the certificate and the private key:

```
openssl pkcs12 -export -out alpha.p12 -inkey alpha.key -in alpha.cer
```

5. Create the client jks file and import the p12 file into it:

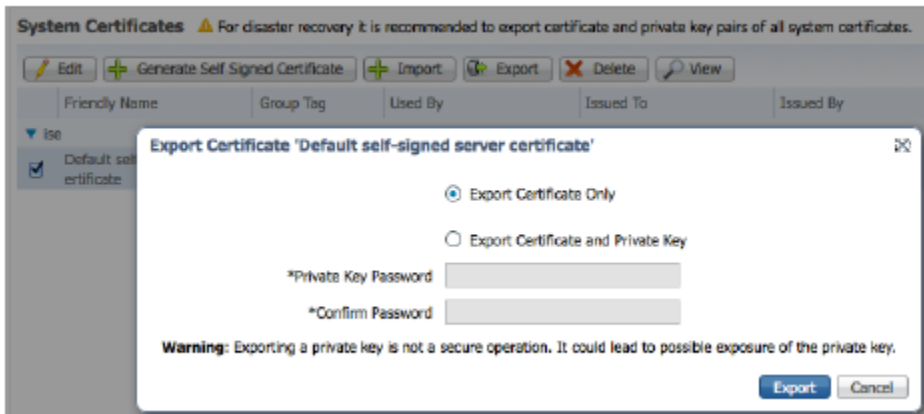
```
keytool -importkeystore -srckeystore alpha.p12 -destkeystore alpha.jks -srcstoretype PKCS12
```

6. Export the public ISE Identity certificate (PEM format):

- A. Connect to the ISE WebUI

- B. Go to *Administration* - go to *System* - go to *Certificates* - expand *Certificate Management* - click on *System Certificates*

- C. Check the default certificate - click on *Export* - select "Export certificate only"



- D. Rename the *.pem file to something more friendly - in our example, we will use "isemnt.pem".

7. Convert the certificate to DER format:

```
openssl x509 -outform der -in isemnt.pem -out isemnt.der
```

8. Add the certificate to the client jks (created in Step 5):

```
keytool -import -alias mnt1 -keystore alpha.jks -file isemnt.der
```

Note: Answer "yes" when asked whether to trust this certificate.

9. Import the pxGrid client certificate into the identity keystore:

keytool -import -alias pxGridclient1 -keystore alpha.jks -file alpha.cer

10. Create the server JKS file:

keytool -import -alias root1 -keystore alpha_root.jks -file isemnt.der

Note: Answer "yes" when asked whether to trust this certificate.

11. Upload the client certificate (alpha.cer) to the ISE Server Trusted certificates:

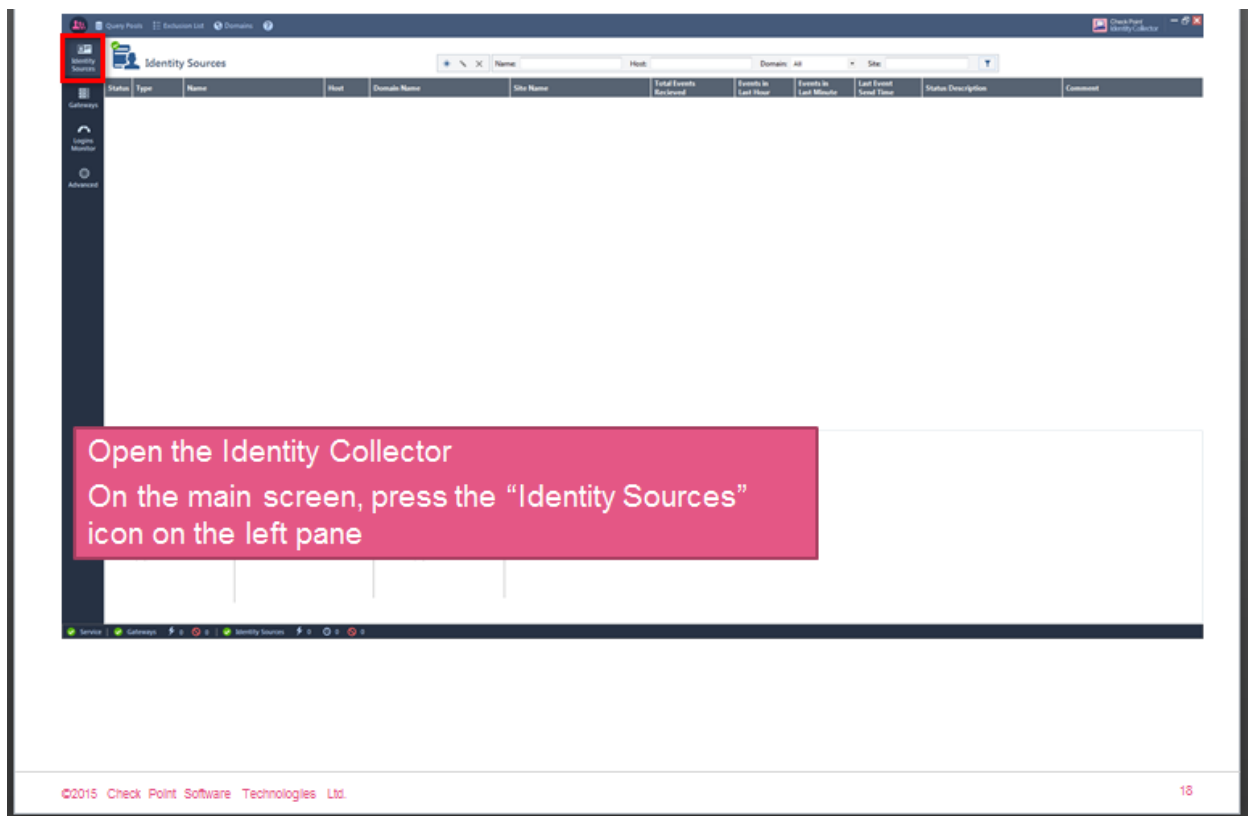
- A. Connect to the ISE WebUI
- B. Go to *Administration* - go to *System* - go to *Certificates* - expand *Certificate Management* - click on *Trusted Certificates*
- C. Click on *Import*

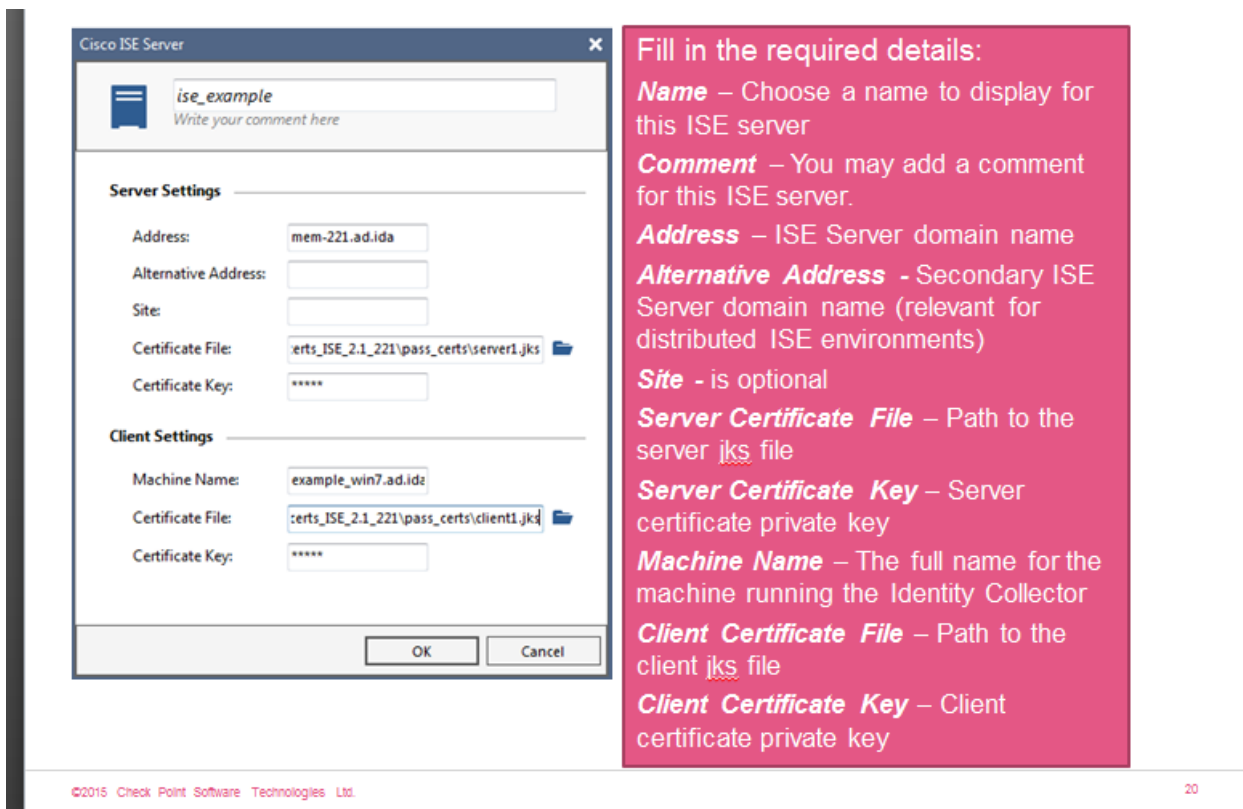
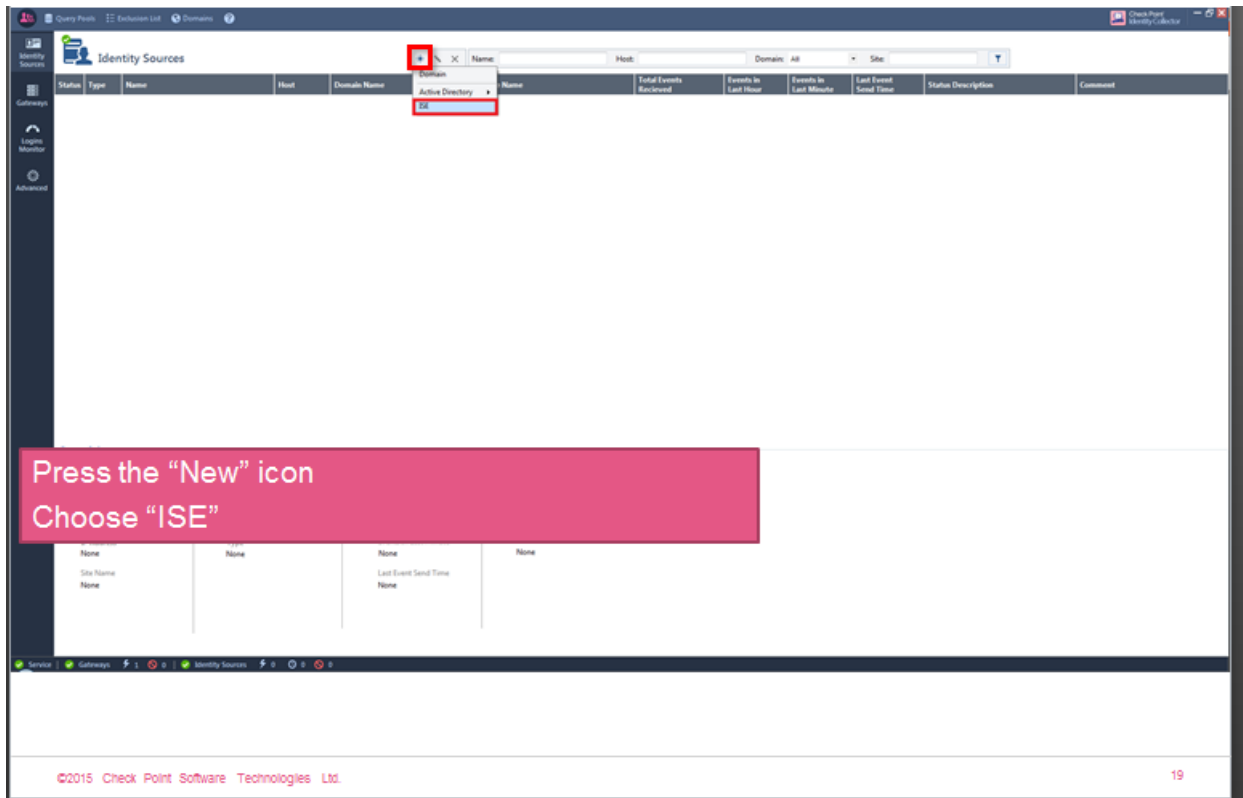
The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. The left sidebar shows a menu with 'Certificate Management' expanded, containing 'Overview', 'System Certificates', 'Endpoint Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', and 'Certificate Periodic Check Settings'. The main content area is titled 'Import a new Certificate into the Certificate Store'. It features a 'Certificate File' field with a 'Browse...' button and the filename 'alpha.cer'. Below this is a 'Friendly Name' text input field. The 'Trusted For' section includes four checkboxes: 'Trust for authentication within ISE' (checked), 'Trust for client authentication and Syslog', 'Trust for authentication of Cisco Services', and 'Validate Certificate Extensions'. A 'Description' text input field is located at the bottom. 'Submit' and 'Cancel' buttons are positioned at the bottom right of the form.

Adding ISE Server to IDC

Before proceeding make sure to locate both the .jks and root.jks files. When configuring the Check Point IDC

- the `alpha.jks` file should be used for client certificate file
- the `alpha_root.jks` file should be used for server certificate file





You should see the newly added ISE Server as "Pending" (Yellow Status)

Status	Type	Name	Host	Domain Name	Site Name	Total Events Received	Events In Last Hour	Events In Last Minute	Last Event Send Time	Status Description	Comment
Pending	Cisco ISE	ise_example	mem-221.ad.ile			0	0	0	---		

Source Info

Hostname ise_example	Status Pending	Total Events Sent 0	Client Machine Name dedy-wm7.ad.ile
Comment	Status Description	Events In Last Hour 0	Server Certificate File D:\vs\ike_project\certs_08_23_2017\psu.com\root2.jks
IP Address mem-221.ad.ile	Type Cisco ISE	Events In Last Minute 0	Client Certificate File D:\vs\ike_project\certs_08_23_2017\psu.com\root2.jks
Site Name		Last Event Send Time ---	

©2015 Check Point Software Technologies Ltd. 21

**Login to the ISE Server WebUI
Choose "Administration" and then "pxGrid Services"**

©2015 Check Point Software Technologies Ltd. 22

You should see the Identity Collector client
 (Note: the client name to look for is the
 “Machine Name”, inserted when you’ve added
 the ISE Server to the Identity Collector)
 Mark the checkbox next to it
 Click “Approve” to approve the Identity Collector
 client machine

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
<input type="checkbox"/> ise-admin-mem-221		Capabilities(4 Pub, 2 Sub)	Online	Administrator	Certificate	View
<input type="checkbox"/> ise-net-mem-221		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
<input checked="" type="checkbox"/> Identity-collector		Capabilities(0 Pub, 0 Sub)	Pending	Session	UserName/Password	View

©2015 Check Point Software Technologies Ltd. 23

The Identity Collector client is now approved in
 the ISE Server and its Status should become
 “Online”

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
<input type="checkbox"/> ise-admin-mem-221		Capabilities(4 Pub, 1 Sub)	Online	Administrator	Certificate	View
<input type="checkbox"/> ise-net-mem-221		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
<input checked="" type="checkbox"/> Identity-collector		Capabilities(0 Pub, 0 Sub)	Online	Session	UserName/Password	View

©2015 Check Point Software Technologies Ltd. 24

Configure Security Gateway Policy

The following guidelines need to be followed when configuring the rule base

- Only access roles can be used when creating an ISE policy
- User group name must match exactly what is in Cisco ISE
- User group needs to have the **CSGT** prefix
- Groups are left empty to be populated automatically
- Access Roles name need to be prefix with **SGT**

User Group

CSGT-POC_Allow
Enter Object Comment

Mailing List Address:

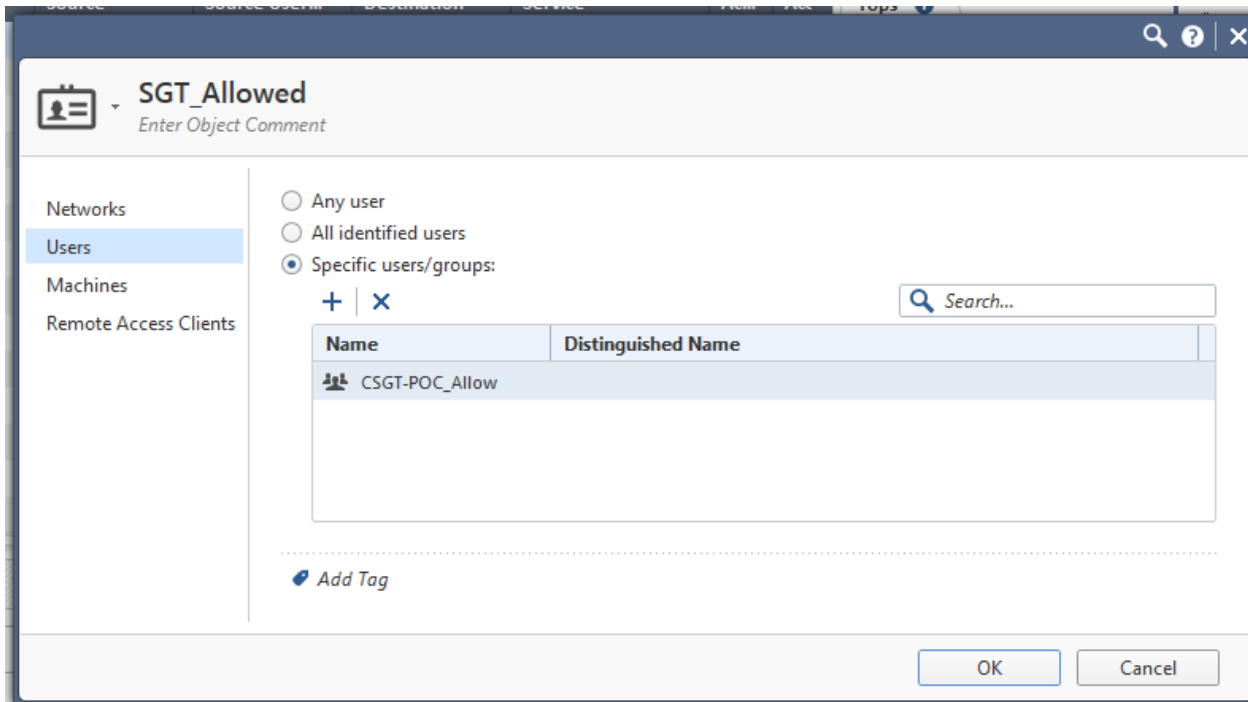
+ | ×

Name	Comments
No items found	

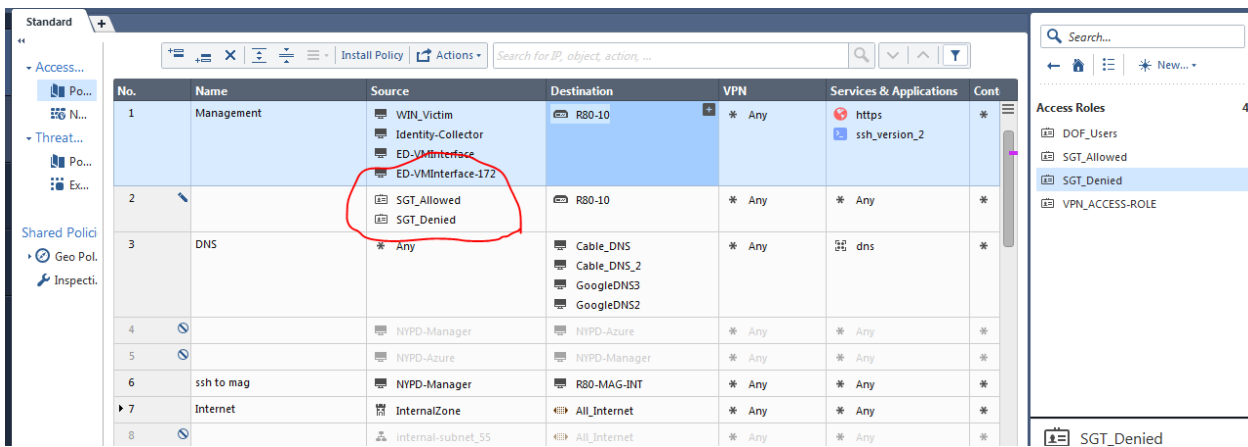
[Add Tag](#)

OK Cancel

Select New, More, User, User Group
Enter a name starting with CSGT-POC_Allow (match name in ISE)



Select New, More, User, Access Role
Prefix the name with SGT_ the group name (Allowed for example)
Select User, Specific users/groups
Select the + and add the newly created empty group (for ex. CSGT-POC_Allow)
Select Ok



Go to Policy and select add rule
Click on the plus and select the Access Role Object
Access Role Object can be either source or destination

Resolving Issues When Something Goes Wrong

Connectivity test failed

New Gateway

gwR80_10
Write your comment here

Server Info

IP Address: 192.168.169.254

Shared Secret: *****

Query Pool: NGTpdemo Data

Pre R80.10 Gateway:

Test ERROR: Refer to [sk113021](#)

Certificate Info

Fingerprint unresolved

Name unresolved

- The gateway uses the IPSec VPN certificate for securing the connection with the Identity Collector.
- This certificate is only created when the IPSec VPN Blade is enabled.

You will find guidelines in [sk113021](#) that refer to the certificate used by the gateway to authenticated and secure the connection.

If for any reason, you need to reestablish the trust between the Identity Collector and the gateway, use the following process

- Disable any ID Awareness configuration on the gateway
 - **Clear the list of “authorized clients”**
- Install policy
- Delete the gateway object on the Identity Collector
- Take a deep breath
- Configure ID Awareness for Identity Collector again on the gateway
 - Add the ID Client host as “authorized client”
 - Copy the shared secret generated
- Add the gateway and use the new generated shared secret
- Be faithful – it will work!

Identity Collector Settings

Client Access Permissions

Client can access this gateway only through internal interfaces

Edit...

Authorized Clients

Client Name	Secret

Selected Client Secret: [] Strong

Generate

Authentication Settings

Settings...

OK Cancel

4. After installing the correct version of Java, it is necessary to restart the Identity Collector service as described in "Appendix A".
5. Check whether the connectivity is restored.
6. Verify that Java ISE extension process is running.

The Java ISE extension is a process that perform the actual communication between the Identity Collector service and the ISE Server.

The Java ISE extension process will not be running, if one of the following occurs:

- The ISE extension debug file does not exists:
%WINDIR%\TEMP\ia_ise_extension.log
- The ISE extension debug file exists but there are no recent debug message.
- The **java.exe** process is not running (does not appear in the process list in the Windows Task Manager).

This check could be tricky because if there is another Java application installed on the machine, it will also be seen as *java.exe* in processes list in the Windows Task Manager.

If the Java ISE extension process is not running, and the installed Java version is correct (see bullet #2 above), then try restarting the Identity Collector service as described in "Appendix A".

If the issue persists, then collect these files and open an investigation Task with CFG:

- ***%WINDIR%\TEMP\ia_****
- ***C:\ProgramData\CheckPoint\IdentityCollector****

Notes:

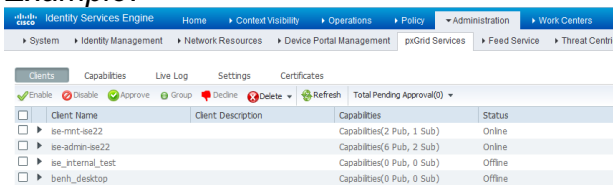
- If none of the conditions above are met, then check the ***%WINDIR%\TEMP\ia_ise_extention.log*** debug file and try to understand the reason of the failure.
If this debug does not provide the relevant information, then collect these files and open an investigation Task with CFG:
 - ***%WINDIR%\TEMP\ia_****
 - ***C:\ProgramData\CheckPoint\IdentityCollector****

Status of the ISE connection - "Pending administrator approval"

Check if the Identity Collector is actually pending for approval on the ISE Server:

- A. Connect to the **ISE Server** WebUI
- B. Go to the **Administration** tab
- C. Go to the **pxGrid Services** tab

Example:



Next steps:

- If an Identity Collector entry exists and pending for approval, then approving it should resolve the issue.
- If an Identity Collector entry exists and it is in "online" state, then try deleting the entry and restarting the Identity Collector service as described in "Appendix A".
- If there is no Identity Collector entry in the **pxGrid Services** list, then there is probably an issue with certificates for the *Identity Collector* <=> *ISE Server* trust.

Try to understand the root cause of the issue from:

- Error messages in the Identity Collector Activity Log (go to **Advanced - Activity Log**)
- ISE Extension debug file - **%WINDIR%\TEMP\ia_ise_extension.log**

If the issue persists, then contact **Cisco support**.

Status of the ISE connection - "Success", but there are no events in the Identity Collector

1. Check if you see the call for the **onChange** function in the ISE extension debug file (**%WINDIR%\TEMP\ia_ise_extension.log**) with the relevant event information from the ISE Server.

The **onChange** function is called whenever an event is received from the ISE Server. The relevant line you should be looking for in the debug file is described in "Appendix B".

2. If you see the relevant **onChange** call in the ISE extension debug file (**%WINDIR%\TEMP\ia_ise_extension.log**), but there are no events in the Identity Collector, then try to understand the reason the event was dropped.

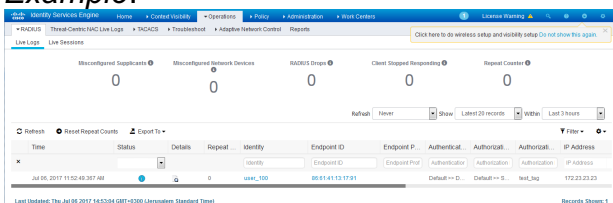
If this debug does not provide the relevant information, then collect these files and open an investigation Task with CFG:

- **%WINDIR%\TEMP\ia_***
 - **C:\ProgramData\Checkpoint\IdentityCollector***
3. If you do not see the relevant **onChange** call in the ISE extension debug file (**%WINDIR%\TEMP\ia_ise_extension.log**), then the ISE Server does not update the Identity Collector on new events for some reason.

Check whether you see the login event on the ISE Server:

- A. Connect to the **ISE Server** WebUI
- B. Go to the **Operations** tab
- C. Go to the **RADIUS** tab
- D. Go to the **Live Logs** section

Example:



Contact **Cisco support** with all the information.

Appendix A

The Identity Collector runs as Windows service.

If you need to restart it, then follow these steps:

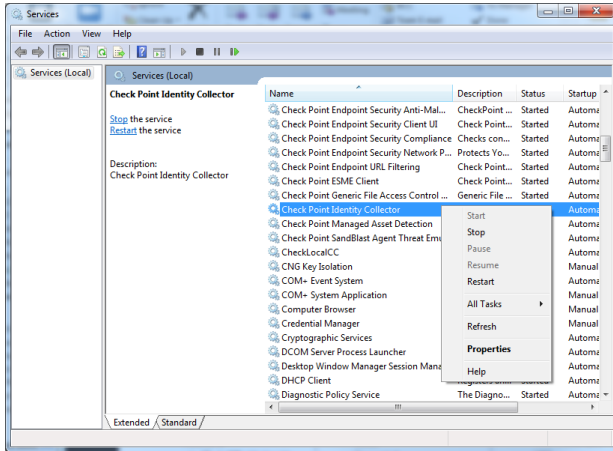
1. Go to the **Start** menu - **Run...** - type **services.msc** and press Enter / click OK
2. Stop the Identity Collector service:

Right-click on the **Checkpoint Identity Collector** - click on **Stop**

3. Start the Identity Collector service:

Right-click on the **Checkpoint Identity Collector** - click on **Start**

Example:



Appendix B

To confirm the event is received in the Identity Collector properly, look for the following lines in the ISE extension debug file (`%WINDIR%\TEMP\ia_ise_extension.log`):

Important Note: Verify that the event information contains a username, or machine name (or both), and machine IP address. If an event does not contain both username and machine name (or machine IP address), it will be dropped!