Certego s.r.l.

Via Ferruccio Lamborghini, 81
41121 Modena MO, Italy
+39-059-7353333

Certego Tactical Response - Cisco ISE configuration

Introduction **1**

Configure ISE **1**
- Enable pxGrid services 1
- Configure ISE to approve all pxGrid certificate-based accounts 3
- Add permissions 4
  - Generate and export pxGrid client certificate 4
- Create ANC Policy and Global Exception 5

Test integration **6**
- Activate account 6
- Test integration 7

Introduction

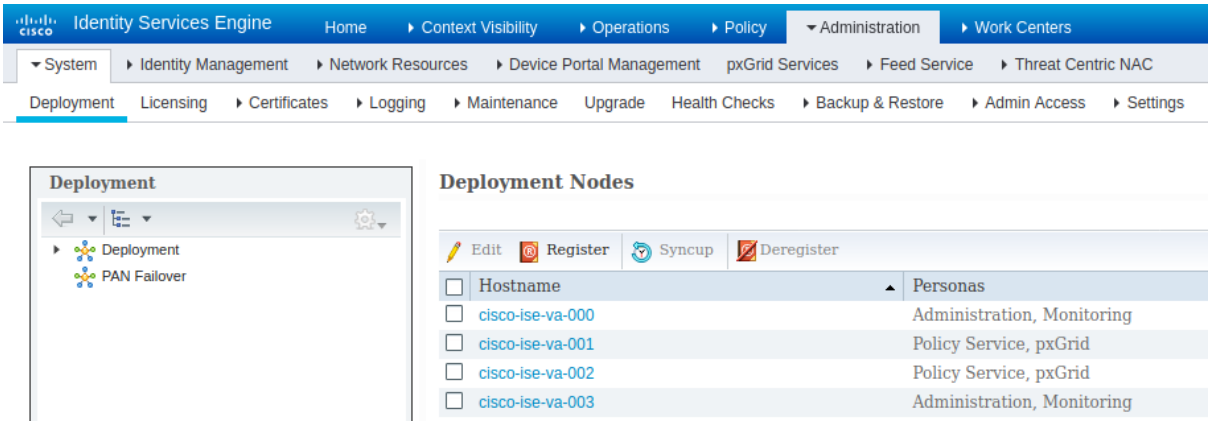
This document describes the required configuration steps to integrate Certego Tactical Response service with Cisco ISE version 2.7, using pxGrid API. It's recommended to stay with the latest patch applied and recommended release of ISE. It should work with ISE 2.4+.

Configure ISE

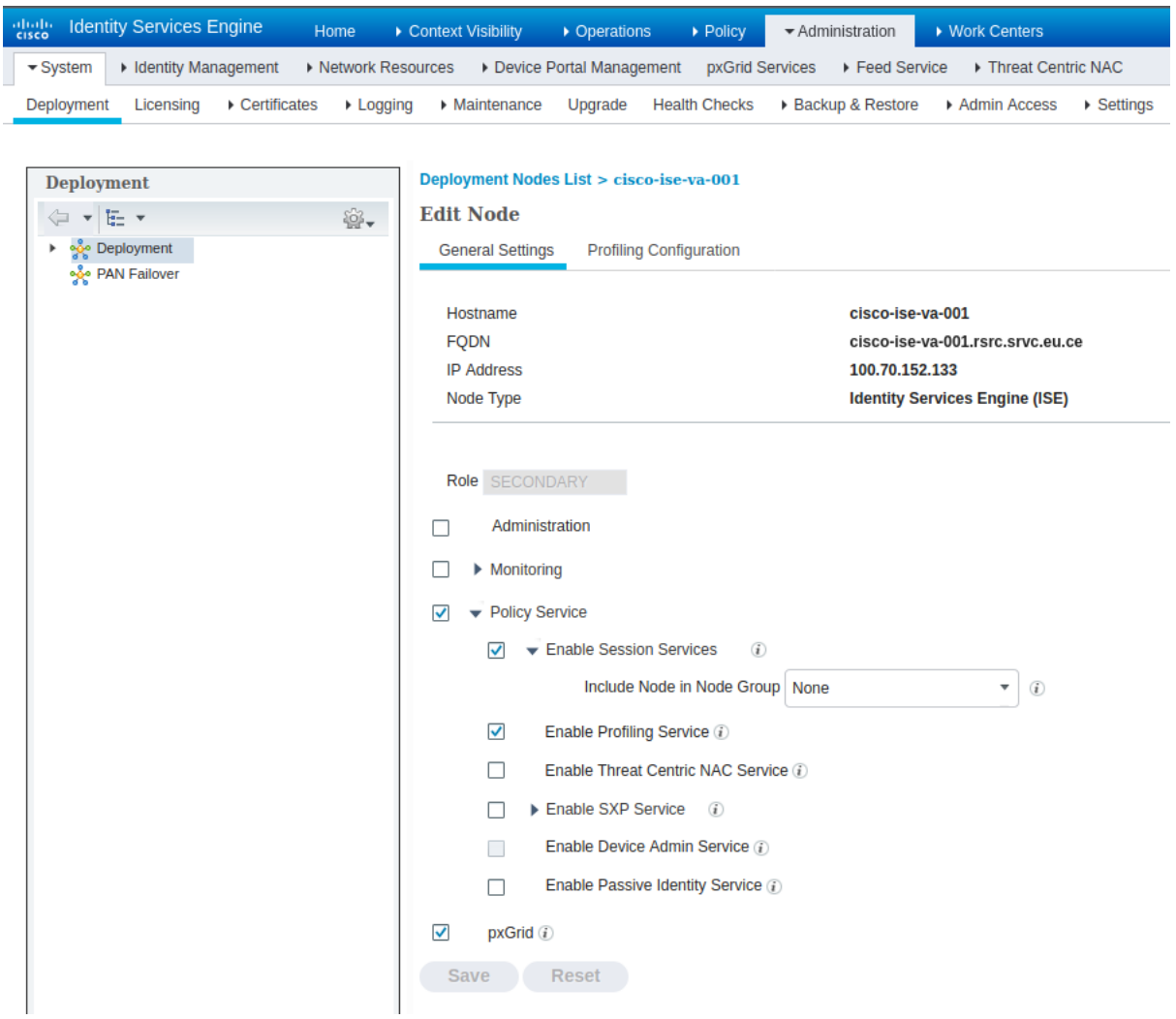
Enable pxGrid services

1. Log into the ISE Admin GUI, navigate to **Administration > Deployment**.

2. Select the ISE node to be used for pxGrid persona as shown in the image.



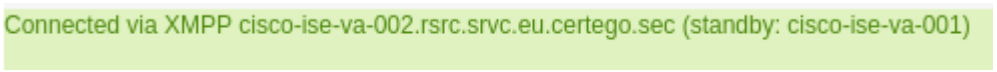
3. Enable pxGrid service and click **Save** as shown in the image.



4. Verify that the pxGrid services are running from the CLI. SSH into the ISE pxGrid node CLI and check the application status. It might take up to 5 minutes for the pxGrid services to fully start and determine High Availability (HA) state if more than one pxGrid node is in use.

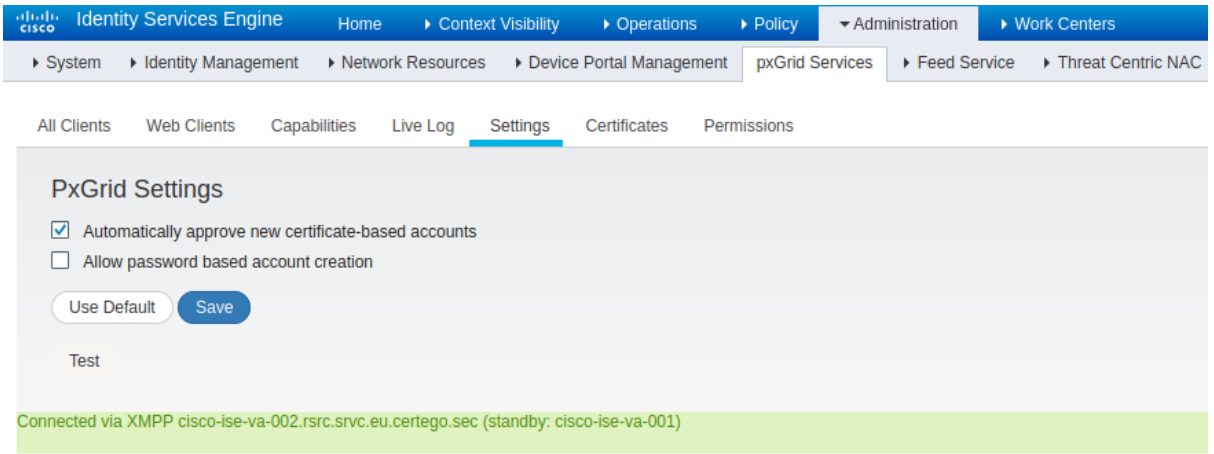
```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

5. Access the ISE Admin GUI and verify that the services are online and working. Navigate to **Administration > pxGrid Services**. At the bottom of the page, ISE should display **Connected to pxGrid <pxGrid node FQDN>** as shown in the image.



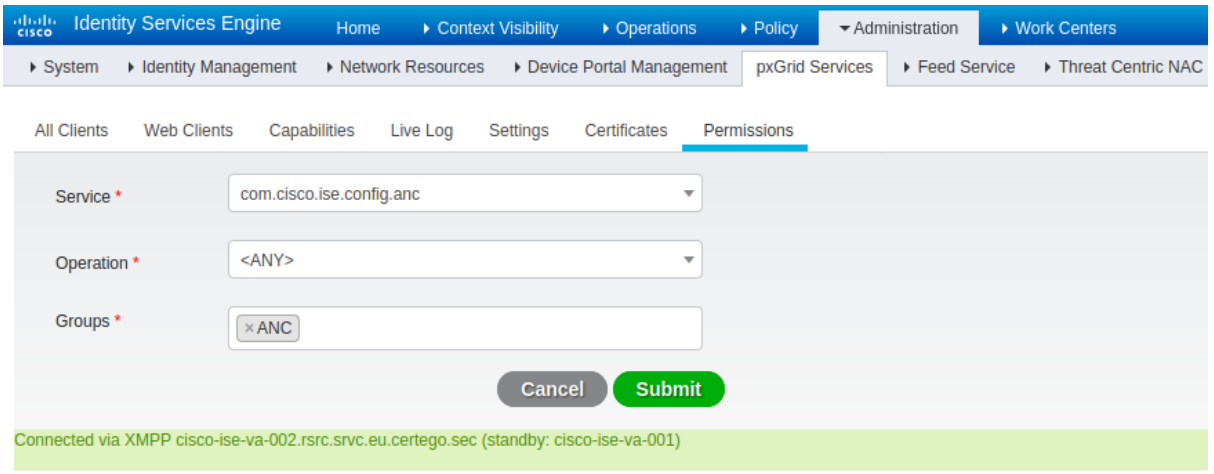
Configure ISE to approve all pxGrid certificate-based accounts

1. Navigate to **Administration > pxGrid Services > Settings**. Check the box "Automatically approve new certificate-based accounts" and click **Save** as shown in the image. If this is not checked, the administrator will have to manually approve the Certego client request.



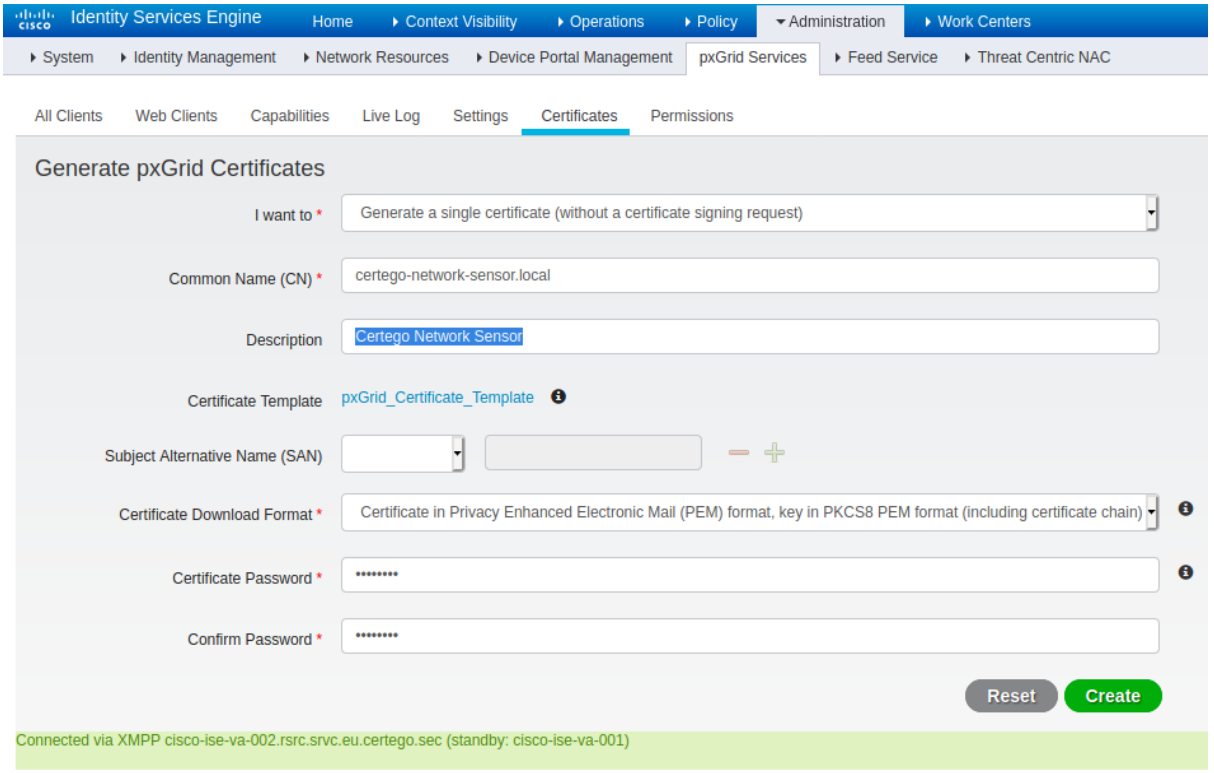
Add permissions

1. Navigate to **Administration > pxGrid Services > Permissions**. Click **Add** to create a permission set which will be used later.



Generate and export pxGrid client certificate

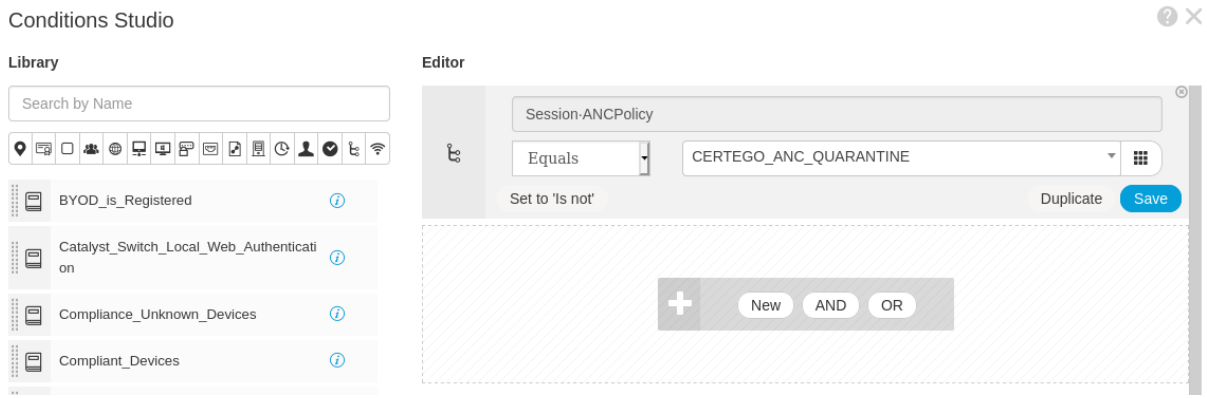
1. Select **Administration > pxGrid Services > Certificates**. Provide the following information. CN name should be Fully Qualified Domain Name (FQDN) resolvable. Optionally, provide a SAN in the form of an IP address or a FQDN. It's recommended that both IP and FQDN are utilized. Also make sure DNS forward and reverse for all systems are made.

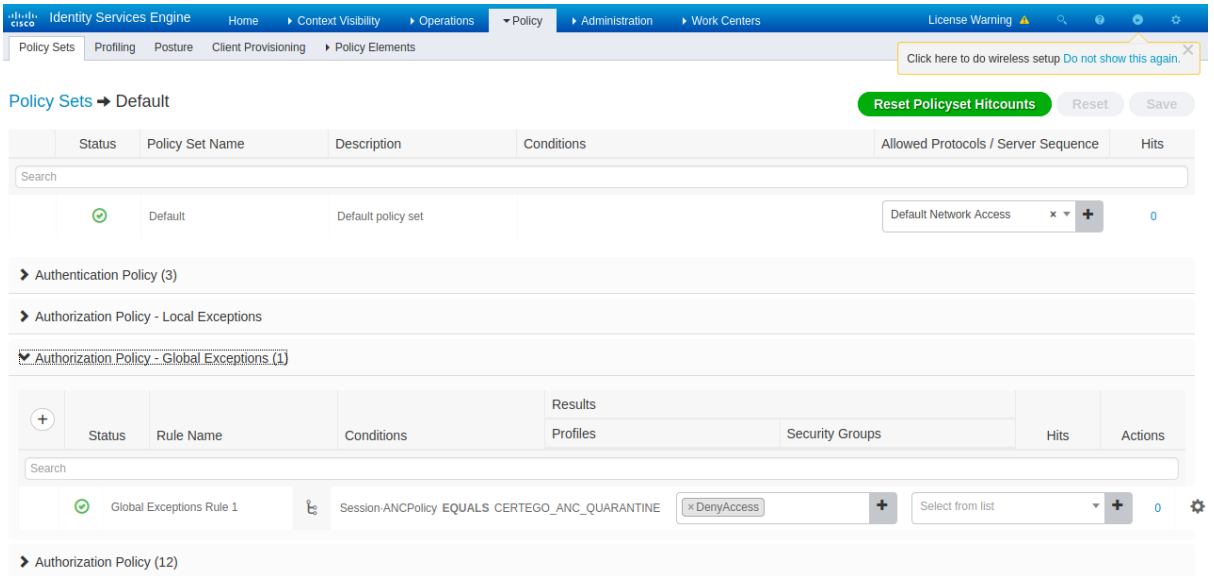


2. Select **Create** and download the zipped file, which needs to be sent to Certego.

Create ANC Policy and Global Exception

1. Navigate to **Operations > Adaptive Network Control > Policy List**. Create a new policy with the name "**CERTEGO_ANC_QUARANTINE**" and action "**QUARANTINE**".
2. Select **Policy > Policy Sets**. Select the required policy set and create a new Global Exception under **Authorization Policy - Global Exceptions** to define how to handle quarantined endpoints. The rule needs to have high priority, otherwise it could be bypassed by other rules.





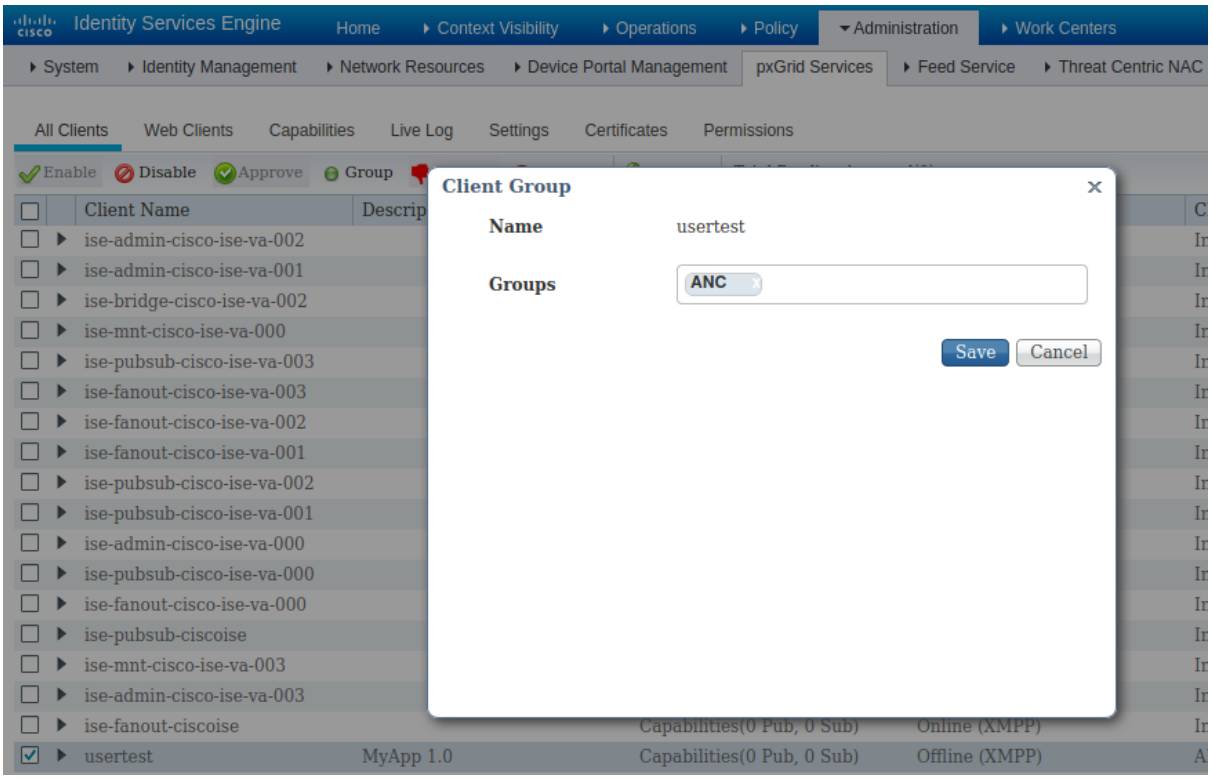
Test integration

Activate account

After configuring ISE, share with Certego IRT the following information:

1. The previously generated pxGrid client certificates and password (which should be sent using an alternative channel for security reasons).
2. ISE's IP address and/or FQDN. Optionally, if a multi-node is being used, this information should be provided also for all the nodes with pxGrid services enabled, to enable high availability. Note: make sure Certego's network sensor can reach ISE.

Ati this point, Certego will perform some HTTP requests to activate the account. The new client should appear under **Administration > pxGrid Services > All Clients**. Select the new account, click on **Group** and assign the **ANC** group.



Test integration

1. Ask Certego to quarantine a test endpoint using the pxGrid integration.
2. Check if the endpoint has been added under **Operations > Adaptive Network Control > Endpoint Assignment**.
3. Check if the endpoint is actually quarantined (i.e. not able to access the network).
4. Ask Certego to remove the blocked endpoint.