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.

dialine Identity Services Engine Home + C	ontext Visibility ► Operations ► Policy <	stration Work Centers		
▼System → Identity Management → Network Reso	urces	Feed Service		
Deployment Licensing + Certificates + Logging	Maintenance Upgrade Health Checks Backup	& Restore + Admin Access + Settings		
Deployment	Deployment Nodes			
💑 PAN Failover	Hostname	▲ Personas		
	cisco-ise-va-000	Administration, Monitoring		
	cisco-ise-va-001	Policy Service, pxGrid		
	cisco-ise-va-002	Policy Service, pxGrid		
	cisco-ise-va-003	Administration, Monitoring		

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

diade Identity Services Engine		ngine _H	Home		 Operations 	Policy	- Administration	Work Centers		
	▼ System	Identity Man	agement 🕨 N	letwork Resou	rces 🔹 🕨 Device F	ortal Managen	ient pxGrid S	Services Feed Se	rvice	
	Deployment	Licensing	 Certificates 	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	e Admin Access Settings	

Deployment	Deployment Nodes List > cisco-ise-va-001	
(= • E • §).	, Edit Node	
 > 양한 Deployment > 양한 PAN Failover 	General Settings Profiling Configuration	
	Hostname cisco-ise-va-001	
	FQDN cisco-ise-va-001.rsrc.srvc.eu.ce	
	IP Address 100.70.152.133	
	Node Type Identity Services Engine (ISE)	
	Role SECONDARY	
	Administration	
	□ ► Monitoring	
	✓ Velicy Service	
	✓ Fnable Session Services (i)	
	Include Node in Node Group None	
	Enable Profiling Service (i)	
	Enable Threat Centric NAC Service (i)	
	□ ► Enable SXP Service (i)	
	Enable Device Admin Service (i)	
	Enable Passive Identity Service (i)	
	V pxGrid (i)	
	Save Reset	

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
#
```

 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.

Connected via XMPP cisco-ise-va-002.rsrc.srvc.eu.certego.sec (standby: cisco-ise-va-001)

Configure ISE to approve all pxGrid certificate-based accounts

 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.

altalta cisco	Ident	ity Services En	gine _H a	me 🕨 Cont	ext Visibility	 Operation 	s ▶P	► Policy		inistration	ork Centers	
▶ Sy	stem	Identity Manag	gement 🕨 N	etwork Resource	s I Devic	e Portal Manage	ment p	oxGrid Se	ervices	Feed Se	rvice	Threat Centric NAC
All	Clients	Web Clients	Capabilities	Live Log	Settings	Certificates	Permissi	sions				
P	xGric	d Settings										
	Auto	matically approve	new certificate	-based accounts								
	Allow	password based	account creati	on								
	Use De	efault Save)									
	Test											
Conne	cted via	A XMPP cisco-ise-	va-002.rsrc.srv	c.eu.certego.sec	: (standby: ci	sco-ise-va-001)						

Add permissions

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

ahaha cisco	Identity Services E	Engine _{Hom}	e ► Conte	xt Visibility	 Operation 	ns	Policy	▼ Adm	inistration	♦ W	ork Centers
► S	ystem 🔸 Identity Mar	nagement 🔹 🕨 Netv	vork Resources	B Devic	e Portal Manag	ement	pxGrid S	Services	Feed Se	rvice	Threat Centric NAC
All	Clients Web Clients	s Capabilities	Live Log	Settings	Certificates	Perm	nissions				
	Service *	com.cisco.ise.con	fig.anc			•					
	Operation *	<any></any>				•					
	Groups *	×ANC									
				Canc	el Subn	nit					
Conne	ected via XMPP cisco-is	se-va-002.rsrc.srvc.	eu.certego.sec	(standby: cis	sco-ise-va-001)						

Generate and export pxGrid client certificate

 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.

dentity Services Engine Hor	ne 🔹 Context Visibility 🔹 C	perations Policy	✓ Administration	Work Centers
System Identity Management Net	work Resources	Management pxGrid Sen	vices Feed Ser	vice
All Clients Web Clients Capabilities	Live Log Settings Certi	icates Permissions		
Generate pxGrid Certificates				
I want to *	Generate a single certificate (wi	hout a certificate signing requ	uest)	v
Common Name (CN) *	certego-network-sensor.local			
Description	Certego Network Sensor			
Certificate Template	pxGrid_Certificate_Template			
Subject Alternative Name (SAN)	•		ŀ	
Certificate Download Format *	Certificate in Privacy Enhanced	Electronic Mail (PEM) format,	, key in PKCS8 PEM	format (including certificate chain)
Certificate Password *	*******			0
Confirm Password *	••••••			
				Reset Create
Connected via XMPP cisco-ise-va-002.rsrc.srvc	eu.certego.sec (standby: cisco-ise-	va-001)		

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.

Con	ditions Studio					Ø ×
Librar	y		Editor			
Sear	ch by Name			Session-ANCPolicy		\otimes
Q 🗔		چ پا 🛇	ĥ	Equals CERTEGO_ANC_QUARANTINE	· III	
	BYOD_is_Registered	(i)		Set to 'Is not'	Duplicate Sa	we
	Catalyst_Switch_Local_Web_Authenticati on					
	Compliance_Unknown_Devices			+ New AND OR		
	Compliant_Devices	<i>i</i>)				

alialia li cisco	dentity	Services	Engine	Home	Contex	t Visibility	 Operations 	▼Policy	Administration	 Work Centers 		License Warning 🔺	্	0	•	¢
Policy S	Sets	Profiling	Posture	Client Provision	ing 🕨	Policy Eleme	nts					Click here to do wireless	setup Do	not sho	v this agai	n.×
Policy	Policy Sets -> Default Reset Policyset Hitcounts Reset Sa															
	Sta	atus	Policy Se	t Name		Description	I	Con	ditions		A	llowed Protocols / Serve	er Seque	nce	Hits	
Search																
	(0	Default			Default polic	y set					Default Network Access	x *	+	0	
> Aut	> Authentication Policy (3)															
> Aut	horizat	ion Polic	y - Local E	Exceptions												
► Aut	horizat	ion Polic	y - Global	Exceptions (1)												
æ									Results							
U	S	Status	Rule Na	ime		Condition	S		Profiles		Security Groups		Hits		Actions	
Sear	ch															
	Ø	Global	Exceptions	Rule 1	Ŀ	Session-AN	CPolicy EQUALS	CERTEGO	_ANC_QUARANTINE	× DenyAccess	+	Select from list		- 4	•	¢
> Aut	horizat	ion Polic	y <mark>(</mark> 12)													

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.

alialia cisco	Identity Services Engine	Home ► Cont	ext Visibility	 Operations 	▶ Policy	▼ Admi	inistration	▶ W	ork Centers	5
► Sy	stem 🕨 Identity Management	Network Resource	s 🕨 Device	Portal Manageme	ent pxGrid S	Services	Feed Se	rvice	Threat	Centric NAC
All C	Clients Web Clients Capabi	iities Live Log	Settings	Certificates F	Permissions					
🖌 En	able 🥝 Disable 🕜 Approve	🖯 Group 📍 Clie	ent Group				• / = 1		×	
	Client Name	Descrip	Nama	1100	tost					C
	ise-admin-cisco-ise-va-002		Name	use	rtest					Ir
	ise-admin-cisco-ise-va-001		Groups	A						In
	ise-bridge-cisco-ise-va-002		oroupo							Ir
	ise-mnt-cisco-ise-va-000						- C		01	Ir
	ise-pubsub-cisco-ise-va-003						Sav	/e	Cancel	Ir
	ise-fanout-cisco-ise-va-003									Ir
	ise-fanout-cisco-ise-va-002									Ir
	ise-fanout-cisco-ise-va-001									Ir
	ise-pubsub-cisco-ise-va-002									Ir
	ise-pubsub-cisco-ise-va-001									Ir
	ise-admin-cisco-ise-va-000									Ir
	ise-pubsub-cisco-ise-va-000									Ir
	ise-fanout-cisco-ise-va-000									Ir
	ise-pubsub-ciscoise									Ir
	ise-mnt-cisco-ise-va-003									Ir
	ise-admin-cisco-ise-va-003									Ir
	ise-fanout-ciscoise			Capabili	ties(0 Pub, 0	Sub)	Online	XMPP)	Ir
	usertest	MyApp 1.0		Capabili	ties(0 Pub, 0	Sub)	Offline	(XMPF	⁽⁾	A

Test integration

- 1. Ask Certego to quarantine a test endpoint using the pxGrid integration.
- 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.