indeni Deployment Checklist

	Pre implementation Configuration	Status
Scope	The following activities should be performed after the indeni server is connected to the network and prior to adding devices for analysis.	
Server Access	Validate access to the indeni server from the relevant user workstations using the following ports: ● TCP 22 (SSH) ● TCP 8181 (web access)	
Server Access validation	Connect your browser to *https://<indeni server IP>:8181* and log in to start your work with indeni (default credentials are: username: 'admin' password: 'admin123!').	
Device Access (Check Point)	Validate access from the indeni server to the relevant devices using the following ports: ● TCP 22 - SSH ● Ping (ICMP Echo)	
User Definition on Devices	Verify that a user is defined on the devices for access by indeni: ● Check Point SecurePlatform - use the bash shell instead of the default. ● Check Point IPSO - uid should be set to 0 (zero), use csh shell and be part of the 'wheel' operating-system-level group. ● Check Point GAiA - use the bash shell, 'adminRole' in Assigned Roles.	

	Initial indeni Administration	Status
Scope	Perform initial administrative configuration of the indeni application Expected duration: 2 hours	
Security	Change passwords for default server users: root & indeni	
Security	Change console password for admin	
Administration	If relevant, integrate with RADIUS or AD	
Administration	Define users for accessing the console	
Device access	Define indeni user on all devices	
Device access	Open ports from indeni to all analyzed devices	
Integration	Enable indeni Insights	
Integration	Define SMTP server and update user's email credentials	
Integration	Define SNMP and/or syslog	
Integration	Define e-mail recipients for alerts	
Integration	Define e-mail alerts level according to user's roles. For example: managers may wish to receive only Critical alerts	
Reports	Define Alert Summary Report	
Reports	Define Procurement Report for device performance and EoL information	
Device Profiles	Define Device Profiles in order to generate compliance alerts	
Device Profiles	Define Device Profile Compliance report	

	Adding Devices	Status
Scope	Add devices for analysis, starting with the management devices followed by the gateways	
Management	Add P1/MDM/Management and wait for discovery	
Management	Add all relevant CMAs and CLMs	
Gateways	If P1/MDM/Management in use, add devices using the “known devices” drop down list	
Gateways	Add standalone devices	
Validation - connectivity	In case of “Failed to Communicate”: check the alert details for the specific reason of the failure (e.g. SSH credentials), fix it and check that the alert is resolved	
Validation - discovery	Check communication status for the devices as displayed by the respective icon (expected: green checkmark and device type)	
Validation - hierarchy	Devices are put into the correct management hierarchy	
Monitoring	Initial alerts are displayed	
Monitoring	Review the alerts that were generated after initial device addition	

	Alert Review and Threshold Tuning	Status
Scope	This activity should be performed about 2 days after the devices were added for analysis followed by at least once a week	
Monitoring	Review new alerts in the console and decide on the required action: ● Fix the issue on the relevant device ● Ignore a specific item that is triggering the alert but is considered irrelevant ● Adjust the threshold that is triggering the alert ● Disable the alert in case it's not relevant for the specific environment	
Monitoring - Failed to Communicate	In case of "Failed to Communicate": check the alert details for the specific reason of the failure (e.g. SSH credentials), fix it and check that the alert is resolved	
Monitoring Suspended	In case of "Monitoring Suspended": check how often this happens. If it happens a lot then check why the relevant device is reaching the CPU and/or memory thresholds	
Resolved Alerts	In case of "Resolved": check the alert's history to see how often the problem is repeated. In case the problem is recurring on a regular basis check for the option of applying the recommended remediation action.	
Reports	Run Inventory report to review device configuration, etc.	

About indeni

Founded in 2009 by a team of network security experts, indeni is revolutionizing networking with the world's first future-proof network management tool. Built on a game-changing platform that combines crowd-sourced knowledge with device-agnostic automated error checking, indeni gives enterprises the high-resolution visibility to preempt costly downtime and service disruption in their networks – while freeing up vital IT resource.

indeni is entrusted by Global and Fortune 100 companies, government agencies and SMBs, to keep their networks running smoothly 24/7/365.

For more information about indeni, visit www.indeni.com or email us at sales@indeni.com.