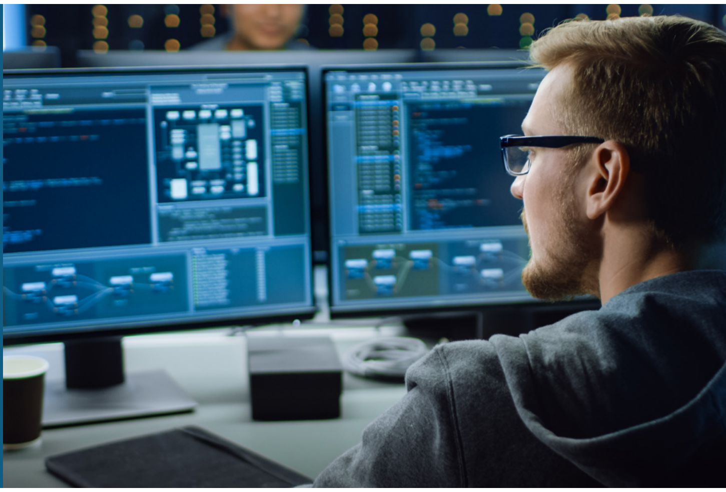
CISCO ISE

SOLUTION BRIEF

Cylera and Cisco ISE Integration

Accelerate Network Access Control Policy Creation

Maximize Cisco ISE investments while improving healthcare IoT device visibility and security



The Challenge

Network Admission Control (NAC) solutions are key to ensuring that only authorized users and devices are granted access to network resources. However, in healthcare and clinical settings, they lack the depth of insight and context required to fully identify all healthcare IoT and connected medical devices and appropriately enforce protective security policies for users and device access control.

Why is this? Many healthcare IoT and connected medical devices are not designed to be managed on the network, and as unmanaged devices, NAC systems have extremely limited visibility into the necessary details that inform suitable action. NAC systems also cannot verify these types of devices' software, firmware, and other details necessary to accurately enforce access and clinical security policies.

Even though NAC solutions can enable preventative protection and enforce efficient authorization and segmentation policies, they require more details and indicators as to why and under what clinical conditions these systems should take specified action. This requires behavioral analytics, baseline device profiling, and an understanding of clinical requirements.

When factored against the range of manufacturers, device and model types, specialized and proprietary protocols, and very little documentation to work with, it's clear that an integration with a solution such as the Cylera platform can make all the difference through clinical risk assessment capabilities and creation of granular policies to restrict and allow the right network access for the right devices at the right times to protect healthcare networks and achieve optimal patient care.

The Integrated Solution

- Cylera has partnered with Cisco to deliver patented techniques and clinical context into its Cisco NAC product, Identity Services Engine (ISE).
- Cylera's healthcare-centric cybersecurity blends intimate knowledge of healthcare IoT device behavior, protocols, medical workflows, patient care, safety, and privacy considerations with Cisco networking and cybersecurity expertise.
- Joint Cylera and Cisco ISE customers can trust that clinical and healthcare professionals can focus on patient care while Cylera provides healthcare IT teams that administer Cisco ISE with enriched visibility and advanced features to allow IT to easily and seamlessly create and either manually or automatically sync error-free policies to ISE.

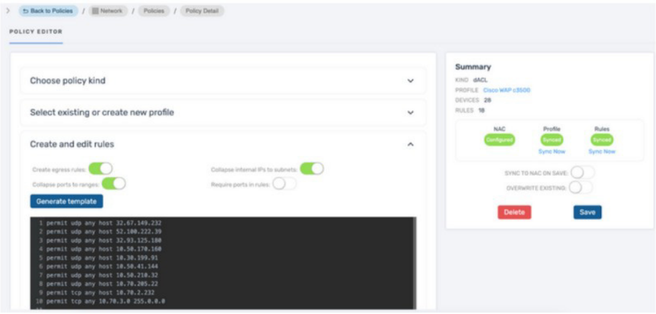
Integrated Solution Benefits

- **Maximize Cisco ISE investments** with Cylera by achieving identity management, access control, and across the whole healthcare enterprise, including healthcare IoT and connected medical devices.
- **Seamless integration** with policy creation, sync with ISE, and Cisco screen views all accessible from the Cylera platform without requiring extra services or backend programming.
- **Save time**, know healthcare IoT and connected medical devices, reduce human error, create and modify Cisco TrustSec and dACL/SGACL policies quickly and without error
- **Zero-touch**, no disruption to physical devices or patient care services, through Cylera passive, patented techniques.

How It Works

Cylera's sensor is easily deployed to monitor network traffic through SPAN or Tap ports on a switch. Connectivity to Cisco ISE and data sharing is through Cisco's Platform Exchange Grid (pxGrid).

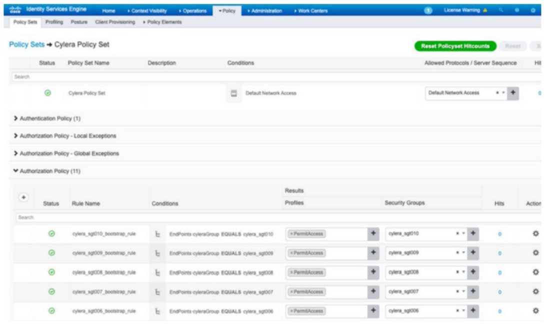
- Cylera's sensor passively monitors network traffic, discovers and profiles IoT, IoMT, and IT/OT assets with zero disruption to patient care services and normal device operations.
- New and updated IoT and IoMT device identification from Cylera is fed into the ISE dashboard, updating its device inventory with granular device information based in deep clinical understanding of operational norms,workflows and risks.
- Within Cylera, administrators can create Cisco TrustSec or dACL/SGACL policies and automatically sync with Cisco ISE.



Summary
KIND dACL
PROFILE Cisco WAP c3500
DEVICES 28
RULES 18

```
permit udp any host 32.67.149.232
permit udp any host 52.100.222.39
permit udp any host 32.93.125.180
permit udp any host 10.50.170.160
permit udp any host 10.30.199.91
permit udp any host 10.50.41.144
permit udp any host 10.50.210.32
permit udp any host 10.70.205.22
permit tcp any host 10.70.2.232
permit tcp any 10.70.3.0 255.0.0.0
```

- Once the policy is sync'd, the Cisco Management Console displays the Cylera policies.



Policy Sets → Cylera Policy Set

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hit
	Cylera Policy Set		Default Network Access	Default Network Access	0

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Action
	cylera_sgt010_bootstrap_rule	EndPoints·cyleraGroup EQUALS cylera_sgt010	PermitAccess	cylera_sgt010	0	
	cylera_sgt009_bootstrap_rule	EndPoints·cyleraGroup EQUALS cylera_sgt009	PermitAccess	cylera_sgt009	0	
	cylera_sgt008_bootstrap_rule	EndPoints·cyleraGroup EQUALS cylera_sgt008	PermitAccess	cylera_sgt008	0	
	cylera_sgt007_bootstrap_rule	EndPoints·cyleraGroup EQUALS cylera_sgt007	PermitAccess	cylera_sgt007	0	
	cylera_sgt006_bootstrap_rule	EndPoints·cyleraGroup EQUALS cylera_sgt006	PermitAccess	cylera_sgt006	0	

Summary

With the Cylera and Cisco ISE integration, healthcare delivery organizations can maximize their Cisco ISE investment while achieving full visibility across their healthcare networks and gain an intimate understanding of the healthcare IoT and connected medical devices on their networks.

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency,mitigate cyber threats, and enable compliance readiness.

CYLERA™

www.cylera.com