Asimily Insight Cisco ISE Integration Guide

Integration details and use cases



Contents

01	Introduction	1
02	Integration Architecture	2
03	Health System Requirements	3
04	Asimily Insight and Cisco ISE Configuration	4
	a. Enable pxGrid Services within Cisco ISE	5
	b. Generate pxGrid certificates for cert-based authentication	6
	c. Configure pxGrid within Asimily Insight	7
	i. Certificate Based Authentication	8
	ii. Password Based Authentication	9
	d. Enable ERS API within ISE	10
	e. Configure ERS API within Asimily Insight	11
05	Integration Use Cases	12
	a. Use Case 1: Device Visibility and Profiling	13
	i. Creating and Importing Profiling Policies	14
	b. Use Case 2: Quarantine Device	15
	c. Use Case 3: Restrict a Service to Reduce Risk from Known Vulnerabilities	16
	d. Use Case 4: Micro-Segmentation based on Neighbor Traffic	17
06	List of Downloadable ACLs	18
	a. Block External Browsing	19
07	Contact	20





01 Introduction

Asimily Insight is a comprehensive medical device cybersecurity and risk management solution that uses multiple information sources including network traffic to solve the following use cases – asset inventory, security risk management, patch prioritization, security and operational alerts, FDA recall monitoring and asset utilization.

Below is an overview of how Asimily Insight maps to the NIST framework

The purpose of this manual is to describe the integration of Asimily Insight with Cisco ISE through various use cases summarized below:

- 01 Device Visibility and Profiling
- 02 Quarantining devices with significant risk
- **03** Restricting a specific network port/service on a device to reduce risk from known vulnerabilities
- 04 Micro-segmentation based on neighbor traffic patterns
- 05 Micro-segmentation based on device profiles



02 Integration Architecture

Asimily Insight integrates with Cisco ISE within the enterprise through the pxGrid controller node (pxGrid API) and the ISE admin node (ERS API). A dedicated Asimily edge appliance or a virtual machine acting as Collector helps Asimily cloud-based portal to connect Cisco ISE and any other third-party vendor platforms deployed within a customer's private network. The Collector must have outbound connectivity with the customer's dedicated portal server in the cloud. The Collector must also have internal connectivity with the required platform such as Cisco ISE.

- 01 Cloud-based Asimily deployment: In a cloud-based deployment, the collector could either be a dedicated appliance provided by Asimily or a Virtual Machine (VM) running inside an enterprise virtual machine platform such as VMware.
- **02** On-premises Asimily deployment: In an on-premises deployment the collector runs within one of the Asimily on-prem servers and there is no need for deploying a dedicated Collector.
- **03** Firewall rule is required to allow the Collector to connect with the customer's portal server in the cloud on TCP ports 5568, 5570, 5572, 5574, 22.

- 04 Connection Security: TLS-based secure connection is used between the Collector and the Asimily server. The connection is initiated by the collector to the Asimily server, which is authenticated using CA-signed certificates. Within the enterprise, the collector connects to the ISE/pxGrid nodes using secure connection. The default and preferred mode of authentication is based on ISE certificates. Alternatively, username/password based authentication is also supported.
- 05 When ISE/pxGrid is deployed in an active/active configuration using two nodes primary and secondary, the Asimily collector automatically reconnects to the remaining active node in case of node failure. Therefore, ISE/pxGrid configuration within Asimily solution requires FQDNs of both nodes.

Figure 1 shows the deployment architecture for Asimily and Cisco ISE.



03 Health System Requirements

Asimily Insight integrates with Cisco ISE within the enterprise. A dedicated Asimily Edge appliance or a Virtual Machine acting as an Edge appliance for Cisco ISE and other platform integrations (i.e. Collector) enables communication between the Asimily server and the Cisco ISE server. See Figure 1 below.

- 01 Cloud-based Asimily Deployment: In a cloud-based deployment, the collector could either be a dedicated appliance provided by Asimily or a Virtual Machine (VM) running inside an enterprise virtual machine platform such as VMware.
- 02 On-premises Asimily Deployment: In an on-premises deployment the collector runs within one of the Asimily on-prem servers and there is no need for deploying a Collector.
- **03** Firewall rule to allow the Collector to connect with the customer's portal server in the cloud on ports 5568, 5570, 5572, 5574, 22.
- 04 Connection Security: TLS-based secure connection is used between the collector and the Asimily server. The connection is initiated by the collector to the Asimily server, which is authenticated using CA-signed certificates. Within the enterprise, the collector connects to the Cisco ISE server.
- 05 One-time action: Connect to the Asimily portal and configure Cisco ISE/pxGrid information FQDNs of pxGrid nodes, method of connection, certificates, authentication information etc. More details on this are in the next section.
- **06** Depending on the use cases detailed in Section 5, there would be a combination of actions within the Asimily portal and Cisco ISE portal that are detailed in that section.



04 Asimily Insight and Cisco ISE Configuration

a. Enable pxGrid Services within Cisco ISE

STEP 1

Navigate to **Administration > Deployment,** select the ISE node to be used for pxGrid, and **check the pxGrid box.**

eployment Licensing + Certi	ficates + Loggi	g Maintenance Upgrade Health Checks	Backup & Restore Admin Access Setti
Deployment		Deployment Nodes List > ise	
G + E +	Q.	Edit Node	
Deployment	20.4	General Settings Profiling Configuration	
PAN Failover			
		FQDN ise.internat.a	simily com
		IP Address 192.168.1.11	
			ices Engine (ISE)
		Other Monitoring Node	
		Enable Session Services (1)	
		Include Node in Node Group	None * (i)
		Enable Profiling Service (j)	
		Enable Threat Centric NAC Service	• 10
		Enable SXP Service (2)	
		Enable Device Admin Service (j)	
		Enable Passive Identity Service ()	
		pxGrid (j)	
	-		

STEP 2

Navigate to **Administration > Deployment,** select the ISE node to be used for pxGrid, and **check the pxGrid box.**



STEP 3

Configure ISE to approve all pxGrid Certificate-Based Accounts: Navigate to **Administration > pxGrid Services > Settings,** and check both boxes show in the figure below.

isco Identit	y Services Eng	jine Hom	e • Contes	t Visibility	Operation	ns I	Policy	▼ Admir	nistration	Work C	Centers
 System 	 Identity Manag 	ement • Netv	ork Resources	+ Devic	e Portal Manag	ement	pxGrid Se	rvices	Feed Service	ce + T	hreat Centric
All Clients	Web Clients	Capabilities	Live Log	Settings	Certificates	Perm	issions				
PxGrid	Settings										
Autom	atically approve r	new certificate-ba	ised accounts								
Allow ;	password based	account creation									
Use Det	ault Save										
Test											
onnected via	XMPP ise.interna	Lasimily.com									

b. Generate pxGrid certificates for cert-based authentication

Navigate to **Administration > pxGrid Services > Certificates,** select the ISE node to be used for pxGrid, and **check** Generate pxGrid Certifications - see figures below. Click Create to download the certificates as a zip file, which will be later required to configure pxGrid within Asimily Insight.

a) Subject Alternative Name (SAN) as FQDN

theter identity Services Engine Hor	me Context Visibility Operations Policy Administration Work Centers
System Identity Management Ne	twork Resources
All Clients Web Clients Capabilities	Live Log Settings Certificates Permissions
Generate pxGrid Certificates	
I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	portal internal asimily.com
Description	Asimily
Certificate Template	pxGrid_Certificate_Template
Subject Alternative Name (SAN)	FQDN portal internal asimity
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chair •
Certificate Password *	••••••
Confirm Password *	
	Reset Create
Connected via XMPP ise internal asimily com	

b) Subject Alternative Name (SAN) as IP Address

dealer Identity Services Engine Ho	me
System Identity Management Ne	twork Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC
All Clients Web Clients Capabilities	Live Log Settings Certificates Permissions
Generate pxGrid Certificates	
I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	portal.internal.asimity.com
Description	Asimity
Certificate Template	pxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 🗸 192.168.1.2 - 🛓
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chair 🗸 0
Certificate Password *	
Confirm Password *	
	Reset Create
Connected via XMPP ise internal asimily.com	

c. Configure pxGrid within Asimily Insight

Figure below is a screenshot of the Connectors Configuration page within Asimily portal. Note Cisco ISE configuration under Network Access Control as either PxGrid or ERS. As mentioned above, Asimily Insight supports both cert-based authentication as well as password-based authentication when connecting to the pxGrid controller node.



i. Certificate Based Authentication (Recommended):

Configuration parameters for certificate based authentication are below:

- 01 pxGrid Node 1* (required): Example: pxgrid1.ise. internal.com:8910 or 192.168.1.11:8910
- 02 pxGrid Node 2 (optional): Example: pxgrid2.ise. internal.com:8910 or 192.168.1.12:8910
- **03** Certificate Password* (required): Password used when generating certificates within ISE. See previous section
- 04 Re-enter Password* (required):
- **05** pxGrid certificate (*.zip)* (required): Upload zip file containing pxGrid certificates generated within ISE as described in the previous section.

Cisco ISE (pxGrid)) Configuration	×
Authentication Type :	Certificate Based Authentication	
pxGrid Node 1 [°] :	• example: pxgrid1.ise.internal.com:8910 or 192.168.1.11:8910	
pxGrid Node 2:	❶ example: pxgrid2 ise internal com:8910 or 182 168 1.11:8910	
Certificate Password [*] :		
Re-enter Password [*] :		
pxGrid certificate (*.zip)*:	Select File	
Synchronization Frequency [*] :	24 hours	
	Cancel	Add

ii. Password Based Authentication:t

Configuration parameters for password based authentication are below:

- 01 pxGrid Node 1* (required): Example: pxgrid1.ise. internal.com:8910 or 192.168.1.11:8910
- 02 pxGrid Node 2 (optional): Example: pxgrid2.ise. internal.com:8910 or 192.168.1.12:8910

Cisco ISE (pxGrid)	Configuration	×
Authentication Type :	Password Based Authentication	
pxGrid Node 1*:		
	• example: pxgrid1.ise.internal.com:8910 or 182.168.1.11:8910	
pxGrid Node 2:		
	example: pxgrid2 ise internal.com:8910 or 192.168.1.11:8910	
Synchronization Frequency	24 hours	
	Cancel	Add



d. Enable ERS API within ISE

ERS (External RESTful Services) API is an optional API that allows automating some of the steps detailed in Use Cases 3, 4, 5 in Section 5. Further information about ERS API can be found in the Cisco ERS API Reference Guide at this link:

https://www.cisco.com/c/en/us/td/docs/security/ise/2- 4/api_ref_ guide/api_ref_book/ise_api_ref_ers1.html#pgfld-1079726

STEP 1

Navigate to Administration > System > Settings > ERS settings > Enable ERS for Read/Write as shown in the figure below.



STEP 2

Navigate to **Administration > System > Admin Access** as shown in the figure below to create an ERS Admin user along with password.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
System Identity Management Identity Management	Vetwork Resources
Deployment Licensing + Certificates	Logging Maintenance Upgrade Backup & Restore Admin Access Settings
Authentication	Administrators List > ers
Authorization	* Name ersadmin
* Administrators	Status 🖉 Enabled 👻
Admin Users	Email
Admin Groups	External (1)
▶ Settings	Inactive account never disabled
	* Password
	* Re-Enter Password
	Generate Password
	♥ User Information
	First Name
	Last Name
	* Account Options
	Description
	▼ Admin Groups
	• BS Adman O +

e. Configure ERS API within Asimily Insight

Configuration parameters for certificate based authentication are below:

- 01 ISE Admin Node 1* (required): Example: ers1.ise.internal.com:9060 or 192.168.1.11:9060
- 02 ISE Admin Node 1* (required): Example: ers2.ise.internal.com:9060 or 192.168.1.12:9060
- **03** Username*: (required)
- 04 Password*: (required)
- 05 Re-enter Password*: (required)



Figure 12: Asimily ISE ERS Configuration

05 Integration Use Cases

a. Use Case 1: Device Visibility and Profiling

Asimily Insight discovers a detailed set of parameters for medical and IoT devices. These include but are not limited to

- Manufacturer, Device Type, Device Model, OS, Software Version, Serial Number
- Impact on Data, Patient, Business; ePHI transmission/ storage; FDA Recalls
- Risk score based on vulnerabilities, exploit analysis, security alerts

Many of the above parameters are not a part of ISE profiler, which has more details on networking infrastructure. Asimily Insight supports ISE Context-In functionality to augment device profile information within ISE. Setting this up requires one-time manual addition of custom attributes listed in the table below to the device profile template in ISE – see figure below. Asimily Insight then automatically populates these attributes for all devices via pxGrid API. Note that Asimily Insight also fetches device profile information from ISE that might not be visible through passive monitoring.

#	Endpoint Custom Attributes (case sensitive)	Data Type
01	asimilyManufacturer	String
02	asimilyDeviceType	String
03	asimilyDeviceFamily	String
04	asimilySoftwareVersion	String
05	asimilyDeviceModel	String
06	asimilyFacility	String
07	asimilyDepartment	String
08	asimilyOS	String
09	asimilyOSFamily	String
10	asimilyHardwareArchitecture	String
11	asimilyStoresEphi	String
12	asimilyTransmitsEPhi	String
13	asimilyRiskScore	Int
14	asimilyHighRiskCveCount	Int
15	asimilyAnomalyPresent	String
16	asimilyFDARecallCount	Int
17	asimilyMDS2Present	String
18	asimilyPatientImpact	String
19	asimilyFDADeviceClass	Int
20	asimilyDataImpact	String
21	asimilyBusinessImpact	String
22	asimilyAcl1	String

tisco iucitu	ty Services Engine	Home	 Context Visibility 	 Operations 		Administration	 Work Centers
 System 	✓ Identity Management	 Network F 	Resources + Device	Portal Management	pxGrid Servic	es + Feed Ser	vice
 Identities 			Identity Source Sequ	vences • Settings	5		
ser Custom A	Hebular	3	Attribu	te name		Туре	
	ation Settings	asin	nilyManufacturer			String *	-
ndpoint Purge		asin	nilyDeviceType			String *) —
ndpoint Custo	m Attributes	asin	nilyDeviceFamily			String -	- [
		asin	nilySoftwareVersion			String *) —
		asin	nilyDeviceModel			String *	
		asin	nilyFacility			String *	-
		asin	nilyDepartment			String *	-
		asin	nilyOS			String *	-
		asin	nilyOSFamily			String -	-
		asin	nilyHardwareArchitectur	e		String *	-
		asin	nilyStoresEPhi			String *) —
		asin	nilyTransmitsEPhi			String *] —
		asin	nilyRiskScore			Int *	-
		asin	nilyHighRiskCveCount			Int •] —
		asin	nilyAnomalyPresent			String *	-
		asin	nilyFDARecallCount			Int •	- [
		asin	nilyMDS2Present			String *	_
		asin	nilyPatientImpact			String *) —
		asin	nilyFDADeviceClass			Int -	-
		asin	nilyDataImpact			String *) —
		asin	nilyBusinessImpact			String -	-
		asin	nilyAd 1			String *	- 0

Figure 13: Define Custom Attributes within ISE

The figure below shows the device parameters that are fed into Cisco ISE through the Context- In functionality.

Identity Services Engine	Home Context Visibility Operations Policy	Administration Work Centers
System Identity Management	letwork Resources	Services + Feed Service + Threat Centric NAC
Identities Groups External Identity	Sources Identity Source Sequences	
Iser Custom Attributes	Attribute name	Туре
Iser Authentication Settings	asimilyManufacturer	String -
ndpoint Purge	asimilyDeviceType	String -
ndpoint Custom Attributes	asimilyDeviceFamily	String -
	asimilySoftwareVersion	String -
	asimilyDeviceModel	String -
	asimilyFacility	String -
	asimilyDepartment	String -
	asimilyOS	String -
	asimilyOSFamily	String -
	asimilyHardwareArchitecture	String -
	asimilyStoresEPhi	String -
	asimilyTransmitsEPhi	String -
	asimilyRiskScore	Int -
	asimilyHighRiskCveCount	Int *
	asimilyAnomalyPresent	String -
	asimilyFDARecallCount	Int -
	asimilyMDS2Present	String -
	asimilyPatientImpact	String -
	asimilyFDADeviceClass	Int -
	asimilyDataImpact	String -
	asimilyBusinessImpact	String -
	asimilyAd 1	String - 🕈

Figure 14: Figure 14: Asimily Device Parameters – Context-In Functionality

The figure below shows the default device parameters displayed within Cisco ISE. Note that these do not include the detailed information provided by the Asimily solution and shown in the previous figure.

Identity Services Engine	Home Context Visibility Operations Policy	
		Services + Feed Service + Threat Centric NAC
	y Sources Identity Source Sequences	
User Custom Attributes	Attribute name	Туре
User Authentication Settings	asimilyManufacturer	String -
Endpoint Purge	asimilyDeviceType	String +
Endpoint Custom Attributes	asimilyDeviceFamily	String -
	asimilySoftwareVersion	String -
	asimilyDeviceModel	String -
	asimilyFacility	String -
	asimilyDepartment	String -
	asimilyOS	String -
	asimilyOSFamily	String -
	asimilyHardwareArchitecture	String -
	asimilyStoresEPhi	String -
	asimilyTransmitsEPhi	String -
	asimilyRiskScore	Int -
	asimilyHighRiskCveCount	Int +
	asimilyAnomalyPresent	String -
	asimilyFDARecallCount	Int -
	asimilyMDS2Present	String -
	asimilyPatientImpact	String -
	asimilyFDADeviceClass	Int -
	asimilyDataImpact	String -
	asimilyBusinessImpact	String -
	asimilyAd1	String - O

Figure 15: Cisco ISE Device Parameters

i. Creating and Importing Profiling Policies

Another **one-time manual step** involves the importing of profiling policies within ISE to associate different groups of devices with their own profiling policy. The next two figures below show examples of profiling policies - one for Medical Devices and another for IoT Devices discovered by Asimily Insight. Within ISE, these new profiling policies can be created under **Policy > Profiling > Profiling Policies.** Notice that the custom attribute, 'AsimilyDeviceFamily', is used in the creation of this profiling policy. These profiling policies are required to be able to enable use cases 3, 4, and 5 discussed further down in this document.

Profiling	Profiler Policy List - Animity_Modical_Device			
Porting Polices Logical Profiles	Policy Enabled * Minimum Cartainty Factor * Exception Action * Nationsk Scare (NMAP) Action Croate an Identity Group for the policy * Parent Policy * Associated CoA Type	50 NONE NONE Image: the state of the state		
	Rules If Cendian CUSTOMATTRIBUTE_	animilyDeviceFamily.	Ceeditions Details CUSTOMANTHEBUTE assimily Deviced analy CONTAINS Medical Devices	<u></u>

Figure 16: Profiling Policy – Asimily Medical Devices

voilling	Profiler Policy List - Avially_Modical_Br	vices		
	Profiler Policy			
2 · E ·	*Ner	w Asimily_Medical_Devices	Description	
Profiling Policies	Policy Enable	e 🖬		A
Logical Profiles	* Minimum Certainty Facto	ar 10	(Valid Range 1 to 65535)	
	* Exception Actio	IN NONE	*	
	* Network Scen (NMAP) Actio			
	Create an identity Group for the pole			
		O No, use existing identity		
	* Parent Polic	NONE	*	
	* Associated CoA Typ	· Clobal Settings		
		e Administrator Created		
	Rules		Conditions Details 2	
	If Condition CUSTOMATTRIBUT	animal Product and a	CUSTOMATTRIBUTE asimily Deviced anily	Q •
	CONTRACT CONTRACT	Construction and	ecosion CONTAINS Modical Devices	
	Save. Renet		•	

Figure 17: Profiling Policy – Asimily IoT Devices

Note that multiple predefined profiling policies from Asimily can be manually imported in an XML file format into ISE without having to create each policy individually. Asimily will provide this XML file during the integration. See "Import" button in the figure below.

Profiling	Profiling Policies			
	<u>م</u>			
(□ + E +		XDdete + @pircort @Eport +		
Prefiling Policies	Profiling Policy Name	 Policy Enabled 	System Type	Description
 Expical Profiles 	2Wre-Device	Enabled	Caco Provided	Policy for 2thre-Device
	C 3Com-Device	Enabled	Caco Provided	Policy for 3Com-Device
	Asstra-Device	finabled	Cisco Provided	Policy for Aastra-Device
	Asstra-IP-Phone	Enabled	Caco Provided	Policy for Aastra-IP-Phone
	Aerohive-Access-Point	Enabled	Caco Provided	Policy for Aerohye-Access-Pont
	Aerohika-Device	Enabled	Caco Provided	Palcy for Aerohive-Device
	American-Power-Conversio	n-Device Enabled	Cisco Provided	Policy for American-Power-Conve
	Andread	Enabled	Caco Provided	Policy for all Android SmartPhone
	Android-Amazon	Enabled	Cisco Provided	Policy for Android Amazon
	Android-Amazon-Kindle	Enabled	Caco Provided	Polcy for Android-Amazon-Kindle
	Androk5-Amazon-Phone	Enabled	Caco Provided	Policy for Android Amszon Phone
	Android-Amazon-TV	Enabled	Caco Provided	Policy for Android Amezon TV
	Androko-Asus	Enabled	Caca Provided	Policy for Android-Asus
	Android-Google	Enabled	Cisco Provided	Palcy for Andraid-Google

Figure 18: Import Profiling Policies

b. Use Case 2: Quarantine Device

For certain security alerts that can pose significant risk like a device browsing malicious domains or an ongoing security attack, quarantining the impacted device might be the fastest solution to contain the risk. Asimily Insight detects high risk security alerts and can immediately take action to quarantine impacted devices through Cisco ISE.

The figure below shows quarantine action being taken from the Asimily portal



Setting this up requires one-time manual creation of ANC policy in ISE as shown in the figure below. Be sure to use "ANC_Quarantine" as the name of this ANC policy.

Figure 19: : Import Profiling Policies

Identity Services Er	ngine Home	Context Visibility	Operations Policy	Administration Work Centers
RADIUS Threat-Centric	NAC Live Logs	TACACS • Troubleshoot	Adaptive Network Cont	ntrol Reports
Policy List Endpoint Assig	Inment			
List > New Input fields marked with an name *	asterisk (*) are require ANC_Quarantine			
Action *	×QUARANTINE)		
			Cancel Sub	mit

In addition, the ANC Quarantine policy created above needs to be associated with an Authorization policy in ISE under Policy > Policy Sets > Authorization Policy (Global Exceptions) as shown in the next two figures below.

	Contraction Contraction Contraction							
Parties Adve Files (Sectorers)	Conditions Studio						0	
Party Sets + Defeat	Library		Editor					CHARLENNED CORD COM
Salar Prilly Set Name	Search by blane			Session AN	Policy			Allowed Property Character Sequence - 1911
	0-3C+0-0-0-8-2E01	0 t 9	ь	Republic	4	Quartere	1.0	
0 and 0	Br00_n_Represed	۲		541 K0 76 K0F			Duplcate Cove	Setur tener room
Y Automation Policy (3)	Cablyst, Darlah, Local, Vela, Autoretical on	0						
• Automation Prop - Local Receptors (1)	Compliance, Unknown, Devices	0				+ New AND OR		
W Auffersteine Pring - Siebel Comptere (II)	Campitent, Devices	٥						
S	EAP-HISCHAPIC	Ø						and the second s
Shink Rule Land C	C 64P.7L3							New York Hand Alleria
2 0. min	G Overst, Ploy	ø						
	MAC, IN, SAM	0						
 Achternan Polity (13) 	Disson, Access, Automation, Passed	0						
	Non_Osco_PhoNest_Phones	ø						
	Nor, Compliant, Devices	0						
	Detth, Local, Mill, Autoretication	10						
	Selet, Web, Automotion	•						
	10 Minut 802.1X	•						
	- 1000 June							
							Chief Use	
		_		_				

Figure 21: ANC Quarantine Authorization Policy – 1

time stanty Services Engine Har	a + Constituting + Operations + Pathy + Advantation + West Const.	Lanes Maring & 1, 8	
Policylan Policy Dokes Cherol	Producenceg + Proby Elements		
Policy Sets + Default		ResetAl Milsourits (Peset)	Seve
Status Policy Set Name	Description Conditions	Allowed Protocols / Server Sequence	1923
Seat			
@ Seast	Soful party set	Debut teranik kulous 🔹 🖷	-
Authentication Policy (3)			
> Authorization Policy - Local Exception	ris [1]		
♥ Authorization Policy - Global Escripti	ens (0)		
		Results	
* Status Rule Name	Conditions	Profiles Security Groups Hits	Actions
Search			
/ @ Quantum	E Design AVCPutry RQMACE Querantive	(Elementation)	0
Authorization Policy (13)			
		Reset	Save

Figure 22: ANC Quarantine Authorization Policy - 2

Figure 20: ANC Quarantine Policy Creation

c. Use Case 3: Restrict a Service to Reduce Risk from Known Vulnerabilities

Asimily has a unique vulnerability management approach that involves discovering vulnerabilities followed by exploit vector analysis and risk assessment. Asimily provides granular recommendations on how vulnerabilities can be mitigated. This allows precise and targeted mitigation of risk posed by vulnerabilities without the need for any patch, which are typically not available immediately or are difficult/time-consuming to apply. In the absence of Asimily recommendations, the alternatives are either to await a manufacturer patch that can lead to prolonged risk exposure or to quarantine or segment the entire device, which can have a negative business impact or is not effective over time.

The figure below shows the various recommendations for a particular device along with a count of vulnerabilities for which each recommendation is applicable.

ASIMILY	Assets Summary Cor	nguration Reports Bookmarks			ធ	۵ و	🚺 admin -
Haemodynam	* ic Recording	Accord Details Topology Vulnerabilities a MDIS2 Impo	at Anomaly Recall Ulika	aton Flow Analysis			
1		Recommendations Application/Device Deputy Poolu	re + MDS2			DEVICE E	POSURE 9
		Q South Passe shiel a servery		📄 Include I	land 🔯	en Hgti Risk	
F	- 60	Pacommendationa	No. Of High Risk CVES	Action			
GE Healthcare Mar	o-Lab	Stop Browsing non-whitelist domains using internet explorer 58 you patch internet explorer or 58 you set internet security zone to high OH 59 you disable active scripting and active X		20			
Device Params		ocentrois					
OUI Manufacturer	Howlett Packard	Stop web browsing non-whitelisted domains And using					
Serial Number		network file share externally And using ernal till you patch OS		×14			
ioftware Version aciity	Facility1						
egartment	angly #	Stop-using Microsoft Edge till you patch or Stop Browsing external websites using Microsoft Edge		A Fix			
ocation		Stop web browsing non-whitelated domains until you patch					
Sub-Modules		CR		¥ Fa			
lardware Architecture		Stop using Microsoft Word till you patch		10			
itores ePHI	-						
hansmits after XMMS to	enety 🖉	Stop uning Microsoft Edge or Internet Englisher till proupetch or Stop browsing external websites using Microsoft Edge or Internet Explorer		≯ Pa			
T Params		Block the download of LNK and PIF files on the Gateway or		20			
P Address	16.20.213.119 (DHCP)	Frend		No. 191			

Figure 23: Recommendations for High Risk Vulnerabilities

The figure below shows detailed information for a specific vulnerability that includes the device configuration trigger, vulnerability exploit vector, recommendations and multiple CVE parameters used in evaluation of the risk score of this vulnerability.



	CVE-2013-3123			*
		Improper Restriction of Operations within the Bours	Is of a Memory Buffer (2.11)	
			ute attackers to anecute arbitrary code or cause a denial of service (memory co mattion Vulnerability," a different vulnerability then CVIC-2013-3111.	
	Device Configuration Trigger:	Device being used for web browsing using internet	ogkrav	
	Vulnerability Exploit Vector:	Web browsing non-whitelisted domains using affect	ed version of internet explorer	
ealthcare Mc				
		Stop Browsing non-whitelet domains using inte OR SII you disable active scripting and active X	met explorer till you patch internet explorer or till you set internet security controle	aone to high
	OVE PARAMETERS			
	Nana		- New -	Value
	Name Confidentiality impact	Ville NCHE	Name Confidentiality Multiplication Factor	Value MEDILM
	Confidentiality impact	NCHE	Confidentiality Multiplication Factor	MERCIN
	Confidentiality impact integrity impact	NCHE HIGH	Confidentiality Multiplication Factor Integrity Multiplication Factor	MEDIAN
	Confidentiality impact integrity impact Availability impact	NCINE HOGH HAIGH	Confidentiality Multiplication Factor Integrity Multiplication Factor Analiability Multiplication Factor	MEDILM MEDILM MEDILM
	Confidentiality Impact Integrity Impact Analizability Impact Attack Weber	NCHE HIGH HIGH NETWORK	Confidentiality Multiplication Factor Integrity Multiplication Factor Analiabity Multiplication Factor Attack Complexity	MEDILAN MEDILAN HAGH LOW

Figure 24: Exploit Vector, Device Configuration Trigger, and Recommendations for a CVE

The figure below shows the ability to select a specific device within the Device View under Mitigation tab in the Asimily portal. The subsequent figure shows the creation of an ACL (access control list) as per Asimily's vulnerability mitigation recommendation, which in this example is to block external browsing from the device.

ASIMILY	Assets Bur	nmary Configuratio	n Reports	Bookmarks						a ¢	0	💽 admin ~
Assot Dotails	Anomaly Vulnarability	es impect Paca	d Utilization	Topology Mitig	tion							Total Court: 1
Categories V	four Device View											₽ Action
9 ==	diress 10.4.20.104											
	P Address	Mac Address	Manufactorer	Device Type	Device Model	05	Facility	Anomaly Score	-	Impact	Likeliho	-
	0 10.4.20.104	00:52:54:95:a6:a2	GE Healthcare	imaging Workstation	-	windows_10	Facility,1	•	•	•	•	
Rows 100	•									1	Proving 1 c	at of 1 records.

Figure 25: Exploit Vector, Device Configuration Trigger, and Recommendations for a CVE

Cess ISE	Block External Browsing			
permit top any 192 168.0.0 0.0 permit top any 192 168.0.0 0.0 permit top any 172 16.0.0 0.15	255,255 eq 443 255,255 eq 40	Î		
permit top any 172 16.0.0 0.15 permit top any 10.0.0 0.256 2 permit top any 10.0.0 0.256 2	55.255 eq 80			
Generale ACL Download	ACL			

Figure 26: Exploit Vector, Device Configuration Trigger, and Recommendations for a CVE

Three manual steps need to be performed within ISE to restrict external browsing:

STEP 1	Create a Downloadable ACL using the auto-generated ACL above.
	The figure below shows the creation of a downloadable ACL through the Cisco ISE portal manually. The ACL generated from the Asimily portal – shown in the previous figure – can be pasted here to generate the downloadable ACL.
STEP 2	Create an authorization profile associated with the above DACL.
	The DACL generated in the previous step needs to be associated with an authorization profile manually as shown in the second figure below.
STEP 3	Create an authorization policy within ISE that applies the above
	authorization profile to a device based on one of its custom attributes.

This is a one-time manual step and is shown in the third figure below.

dentity Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers	
Policy Sets Profiling Posture	Client Provisioning Policy Elements	
Dictionaries + Conditions - Res		
Authentication	Downloadable ACL List > OnlyInternalittpAccess Downloadable ACL	
* Authorization	* Name OnlyInternalHttpAccess	
Authorization Profiles	Description Only allow internal access for HTTP (80) and HTTPS (443)	
Downloadable ACLs		
Profiling	* DACL Content 1234567 permit top any 192.168.0.0.0.0.255.255 eq 80 19310111 permit top any 192.168.0.0.0.0.255.255 eq 443 2131415 permit top any 172.16.0.0.15.255.255 eq 80	
+ Posture	1617161 permit top any 172.16.0.0 0.15.255.255 eq 443 9202122 permit top any 10.0.0.0 0.255.255 eq 80	
Client Provisioning	2324252 permit top any 10.0.0 0.255255255 eq 443 6272829 deny top any any eq 80 3031323 deny top any any eq 443 3343536 permit ip any any 3738394	
	Check DACL Syntax	T.
	Save Reset	

Figure 27: Creation of Downloadable ACL

dualse Identify Services Engine	Home + Context Visibility + Operations + Policy + Administration + Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Elements
Dictionaries + Conditions • Resu	Rs .
Authentication	Authorization Profiles > ONLY_INTERNAL_HTTP_ACCESS Authorization Profile
- Authorization	*Name ONLY_INTERNAL_HTTP_ACCESS
Authorization Profiles	Description
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
+ Profiling	Network Device Profile data Cisco 💌 🕀
+ Posture	Service Template
Client Provisioning	Track Movement 📰 🕢 Passive Identity Tracking 📰 👔
	Common Tasks DACL Name OnlyInternaHttpAccess ACL (Fiter-ID) Security Group VLAN

Figure 28: Create Authorization Profile and associate with DACL

hele Identity Services Engine	Home Context Visibility Opera Client Provisioning Policy Dements	Abro +Policy + Administration + Work Centers		License Warning 📥	9. O	• •
Forty sets Training Tourse	construction of the second					
Policy Sets + Default					Reset	Save
Status Policy Set Name	Description	Conditions		Allowed Protocots / Ser	ver Sequenc	e Hits
Search						
O Default	Default policy set.			Default Network Access	** +	115
Authentication Policy (3)						
Authorization Policy - Local Ex	ceptons (1)					
•			Results			
Status Rule Name	Conditions		Profiles	Security Groups	HIS	Actions
Search						
Ontentional-Hp	Access E EndPoints asimity	Add EQUALS One_Imemal_HTTP_Access	+ ONLY_INTERNAL_HTTP_ACCES	Send fornial	•	0
Authorization Policy - Global E	sceptions					
Authorization Policy (13)						
					Reset	Seve

Figure 29: Create Authorization Policy and associate with Authorization Profile

d. Use Case 4: Micro-Segmentation based on Neighbor Traffic

Asimily Insight discovers and monitors traffic patterns between devices. It also provides a navigable topological view of the network to visualize traffic patterns. Flow analysis tab for each device is another way to visualize the peer IPs for each service used by a device.

The solution allows one to identify the flow of ePHI within the network. It also allows identification of devices that store ePHI, which is discovered by parsing/associating MDS2 documents. In this use case, policy enforcement could involve restricting traffic between known neighbors. To accomplish this, perform the following actions within the Asimily portal

- 01 Identify neighbors by monitoring traffic patterns in the Topology tab see Figure 30.
- 02 Select a device and its neighbors to enforce traffic restriction see Figure 31 and Figure 32.
- **03** Auto-generate ACL based on selected device and neighbors see Figure 33 and Figure 34.

The steps to create downloadable ACL, to create an authorization profile associated with the ACL, and to create an authorization policy are similar to those in Use case 3.

ASIMILY	usets Summary Configure	slon Reports Bookmarka	A 0	🚺 admin ~
Ultrasound	*	Asset Details Tapology Volvenbillies + MD02 Impact Anonety Recal Utilization Imaging Utilization Plan Analysi		
-		One Day One Week	Al Time 🛛 - Legend	•
GE Healthcare Volu	son E8		MAG	-
Device Params		10.4.12.29		
00 Merufacturer	Advantech Technology (CHINA) Co. Ltd.	17 Workstation	540	-
Serial Number		10 181 96.4	Most recent	-
Software Version		thread	nebetrieing device ritz	
Facility	Facility.1	10.20.209.171	Dente with anomaly	
Department		basing Workstation 0 545-111199		
Location		b) 18/ 111 19)		
Sub-Modules				
Hardware Architecture				
Stores of 14	-			
Tanania ePie	-			
CMMSIN				
IT Params				
P Address	10.20.209.171			
	(DHCP)			

Figure 30: Device Topology

ASIMILY Assets Bur	nmary Configuration	n Reports	Bookmarks						П	۵	0	🗊 admin ~
Asset Deballs Anomaly Vulnerability	n Impact Recal	Utilization	Teoringy Million	lan -								Total Count: 1
Categories View Device View												₽ Action
Q #Address: 30.35.398.171 x												
P Address	Mac Address	Manufacturer	Device Type	Device Model	05	Facility	Anomaly Score	- Mak	Imper	•	Ukelhood	
0 10.20.209.171	00.00x00.9438.cc	OE Healthcare	Ubssound	Voluson EB	windows	Facility,1						
Rows 100 *											howing 1.	at of 1 records.

Figure 31: Mitigation – Device View

ASIMILY	Assets Summ	ery Configuration	Reports	Bookmark					R	۵	0	🚺 admin ~
Asset Details Ar	onaly Vuherabilities	Ingest Recal	Unication	Teoringy	Migatori							Total Count: 2
Comparen Ver												Co Back
E Oltra												
		10.20.209.171						00:0kub/94-38cm				
		GE Healthcare						Ultracond				
	Device Model :	Volueon EB						windows				
	Facility :	Pacify_1										
_												Action
Q Teach												
NEIGHBO	RING DEVICE											
	P Address	Mac Add	***		Aurolacturer	Device Type	Device Model	05		Factor	¥	
	010101.111.190				E Healthcare	Imaging Workstation	VewPeid	uninown		Facilit	ty_1	
	• 10,161,96.4	00.50.561	k:76.0b		Marans, Inc.	IT Workstation		windows		Facilit	9.1	
Ross 100 *										9	howing 2	out of 2 necords.

Figure 32: Mitigation – Device Topology View

ASIMILY	Anna Soren	ey Configuration	Take Action	and a		×	R Ó	0	atrin ~
				•	Book External Browsing				
E Ultras									
			Generate ACL						

Figure 33: Device Topology View – Take Action

		Take Action				
				nia Naglav Tafa 🔹		
Congress Ves			ny eq 53 10.361.111.193		ļ	
		Generate ACL	Download ACL			

Figure 34: Device Topology View – Restrict Neighbor Traffic ACL

e. Use Case 5: Micro-Segmentation based on Device Profiles or Device Attributes

As mentioned earlier, Asimily Insight discovers a detailed set of parameters for medical and IoT devices. These include device profile or device type and other device attributes like device family, operating system, device model, manufacturer etc. Network segmentation policies can be enabled on ISE based on these parameters

Policy creation is a one-time manual step and as devices are discovered the policies are automatically applied. For example, all infusion pumps could be grouped into a dedicated VLAN – shown in Figure 35, Figure 36, and Figure 37. Once again, the steps to create downloadable ACL, to create an authorization profile associated with the ACL, and to create an authorization policy are similar to those in Use case 3.

In another example, all imaging devices with specific windows operating systems could be grouped into a dedicated VLAN – as shown in Figure 38.

ASIMILY	Assets Summary Configuration	Reports Bookmarks		R	۵	e 🕐 admin ~
Asset Details Ar	omaly Vulnorabilities impact Rocal	Utilization Topology Miligation				Total Court. 65
Categories View	Davice View					Action
	Device Type		Number Of Devices			
	Infusion pump		4508			
	IT Workstation		1086			
	Medical Device		858			
	Call Station		555			
	Vital Signa Monitor		505			
	Utrasound		259			
	Central Monitoring Station		194			

Figure 35: Mitigation – Category View

then identity Services Engine	Hann + Contret Visibility + Operations • Policy + Astronostration + Walk Centers	Luones Warning 💩 🔍 🔍 🔍 🔍 🔍
PolicySets Profiling Posture	e DestPosisioning +Polo Benerits	
Dictionaries + Conditions	Reads	
	Authoritation Profiles 5 New Authoritation Profile	
> Authentication	Authorization Profile	
* Authorization	*Name latison_Pumps	
Authorization Profiles	Description VARy for Influence Pumps	
Downloadable ACLa	*Access Type ACCESS_ACCEPT +	
* Profiling	Network Device Profile 👜 Claca 🔹 🕀	
+ Postare	Denico Template	
+ Client Provinioning	Track November 1 1	
	Passive Identity Tracking 🔄 (
	* Common Tasks	
	Z CACL Rame FERRIT_ALL_TRATE:	
	E xa.	
	C Decurity Group	
	Z VLAN Tag D 1 (888, 199) DAtama (201	*
	Advanced Attributes Settings	
4 (A	

Figure 36: Create Authorization Profile – Assign VLAN ID

the identity Services Engine Home	Context Visibility + Operations	*Policy + Administration	+ Work Centers		License Warning 📥 🔍	
Policy Sets Profiling Posture Client Provision	ning + Policy Elements					
Status Policy Set Name	Description	Conditions			Allowed Protocols / Server :	Sequence Hits
Dearch						
Ø Default	Default policy set				Default Network Access	* * * 941
Authentication Policy (3)						
♥ Authorization Policy - Local Exceptions (1)						
				Results		
(+) Status Rule Name	Conditions			Profiles	Security Groups	Hts Actors
Search						
Infusion Partips VLAN	b EndPoints asimt/Device	Tipe EQUALS Whaten pump		(+Infusion_Pumps)	Selection tail • +	• •
Authorization Policy - Global Exceptions						
Authorization Policy (13)						
						Reset Save

Figure 37: Create Authorization Policy – Infusion Pumps on specific VLAN ID

MIL	Y Assets S	lummary Configural	ion Reports	Bookmarks						п 4	• •
Details	Anomaly Vulnerab	ittes inpect Po	eal Ulbalor	Tuology M	gation						Total Court
atagories	View Device View										₽ Actio
0	ovice Family : Imaging Devic	na i OS i ulindova i i									
	P Address	Mat Address	Manufactoriar	Device Type	Device Model	ce	Facility	Anomaly Score	Mak .	impact	Likelhood
	• 9234195178	e:01:/7390d/8	GE Healthcare	imaging Workstation	Xeleris	windows	Facility,1				
	• 10.24 196 173		FLUIFILM Corporation	X-Ray		windows	Facility_1				
	●10.28.116.84	14.02.05.ed.te.44	FLUFILM Corporation	Digital Radiography		windows	Facility.1				
	● 10.24.115.171		FLUFFLM Corporation	xAuy		windows	Facility,1				
	•10.28.116.28	00.43.93.97.54.38	GE Healthcare	Ultrasound	LOGIQe	windows	Facility.1				
	• 10/24-202.32	6885849e17.75	Del Inc.	imaging Workstation		windows	Facility.1				

Figure 38: Select Imaging Devices with Windows OS

06 List of Downloadable ACLs

Below is a list of downloadable ACLs that can be created one-time manually within Cisco ISE at the start of Asimily Insight and Cisco ISE integration. For each DACL, a corresponding authorization profile and an authorization policy will also need to be created manually.

a. Block External Browsing

Downloadable ACL

- permit tcp any 192.168.0.0 0.0.255.255 eq 80
- permit tcp any 192.168.0.0 0.0.255.255 eq 443
- permit tcp any 172.16.0.0 0.15.255.255 eq 80
- permit tcp any 172.16.0.0 0.15.255.255 eq 443
- permit tcp any 10.0.0.0 0.255.255.255 eq 80
- permit tcp any 10.0.0.0 0.255.255.255 eq 443 deny tcp any any eq 80
- deny tcp any any eq 443
- permit ip any any

Authorization Policy rule

asimilyAcl1 EQUALS Block_External_Browsing

b. Block RDP

Downloadable ACL

- deny tcp any any eq 3389
- deny udp any any eq 3389
- permit ip any any

Authorization Policy rule

• asimilyAcl1 EQUALS Block_RDP

c. Block SNMP

Downloadable ACL

- deny tcp any any eq 161
- deny tcp any any eq 162
- deny udp any any eq 161
- deny udp any any eq 162 permit ip any any

Authorization Policy rule

• asimilyAcl1 EQUALS Block_RDP

d. Block Network File Share

Downloadable ACL

- deny tcp any any eq 137
- deny tcp any any eq 138
- deny tcp any any eq 139
- deny tcp any any eq 445
- deny tcp any any eq 2049
- deny udp any any eq 137
- deny udp any any eq 138
- deny udp any any eq 139
- deny udp any any eq 445
- deny udp any any eq 2049
- permit ip any any

Authorization Policy rule

• asimilyAcl1 EQUALS Block_NFS

e. Block FTP

Downloadable ACL

- deny tcp any any eq 20
- deny tcp any any eq 21
- deny udp any any eq 20
- deny udp any any eq 21
- permit ip any any

Authorization Policy rule

• asimilyAcl1 EQUALS Block_FTP

f. BBlock Network File Share Externally and Email

Downloadable ACL

- permit tcp any 192.168.0.0 0.0.255.255 eq 137
- permit tcp any 192.168.0.0 0.0.255.255 eq 138
- permit tcp any 192.168.0.0 0.0.255.255 eq 139
- permit tcp any 192.168.0.0 0.0.255.255 eq 445
- permit tcp any 192.168.0.0 0.0.255.255 eq 2049
- permit tcp any 192.168.0.0 0.0.255.255 eq 20
- permit tcp any 192.168.0.0 0.0.255.255 eq 21
- permit tcp any 172.16.0.0 0.15.255.255 eq 137
- permit tcp any 172.16.0.0 0.15.255.255 eq 138
- permit tcp any 172.16.0.0 0.15.255.255 eq 139
- permit tcp any 172.16.0.0 0.15.255.255 eq 445

- permit udp any 172.16.0.0 0.15.255.255 eq 2049
- permit udp any 172.16.0.0 0.15.255.255 eq 20
- permit udp any 172.16.0.0 0.15.255.255 eq 21
- permit udp any 10.0.0.0 0.255.255.255 eq 137
- permit udp any 10.0.0.0 0.255.255.255 eq 138
- permit udp any 10.0.0.0 0.255.255.255 eq 139
- permit udp any 10.0.0.0 0.255.255.255 eq 445
- permit udp any 10.0.0.0 0.255.255.255 eq 2049
- permit udp any 10.0.0.0 0.255.255.255 eq 20
- permit udp any 10.0.0.0 0.255.255.255 eq 21
- deny tcp any any eq 137 deny tcp any any eq 138 deny tcp any any eq 138 deny tcp any any eq 139 deny tcp any any eq 2049 deny tcp any any eq 20 deny tcp any any eq 20 deny tcp any any eq 2 deny udp any any eq 137 deny udp any any eq 138 deny udp any any eq 139 deny udp any any eq 445 deny udp any any eq 2049
 - deny udp any any eq 20
 - deny udp any any eq 21

permit ip any any

Authorization Policy rule

• asimilyAcl1 EQUALS Block_External_NFS

9. Block External Browsing and RDP

Downloadable ACL

- permit tcp any 192.168.0.0 0.0.255.255 eq 80
- permit tcp any 192.168.0.0 0.0.255.255 eq 443
- permit tcp any 172.16.0.0 0.15.255.255 eq 80
- permit tcp any 172.16.0.0 0.15.255.255 eq 443
- permit tcp any 10.0.0.0 0.255.255.255 eq 80
- permit tcp any 10.0.0.0 0.255.255.255 eq 443
- deny tcp any any eq 80
- deny tcp any any eq 443
- deny tcp any any eq 3389
- deny udp any any eq 3389
- permit ip any any

Authorization Policy rule

asimilyAcl1 EQUALS Block_External_Browsing_And_RDP

h. Block ICMP

Downloadable ACL

- deny icmp any any
- permit ip any any

Authorization Policy rule

• asimilyAcl1 EQUALS Block_NFS

i. Block FTP

Downloadable ACL

- permit tcp any 192.168.0.0 0.0.255.255 eq 80
- permit tcp any 192.168.0.0 0.0.255.255 eq 443
- permit tcp any 192.168.0.0 0.0.255.255 eq 137
- permit tcp any 192.168.0.0 0.0.255.255 eq 138
- permit tcp any 192.168.0.0 0.0.255.255 eq 139
- permit tcp any 192.168.0.0 0.0.255.255 eq 445
- permit tcp any 192.168.0.0 0.0.255.255 eq 2049
- permit tcp any 192.168.0.0 0.0.255.255 eq 20
- permit tcp any 192.168.0.0 0.0.255.255 eq 21
- permit tcp any 172.16.0.0 0.15.255.255 eq 80
- permit tcp any 172.16.0.0 0.15.255.255 eq 443
- permit tcp any 172.16.0.0 0.15.255.255 eq 137
- permit tcp any 172.16.0.0 0.15.255.255 eq 138
- permit tcp any 172.16.0.0 0.15.255.255 eq 139
- permit tcp any 172.16.0.0 0.15.255.255 eq 445
- permit tcp any 172.16.0.0 0.15.255.255 eq 2049
- permit tcp any 172.16.0.0 0.15.255.255 eq 20
- permit tcp any 172.16.0.0 0.15.255.255 eq 21
- permit tcp any 10.0.0.0 0.255.255.255 eq 80
- permit tcp any 10.0.0.0 0.255.255.255 eq 443
- permit tcp any 10.0.0.0 0.255.255.255 eq 137
- permit tcp any 10.0.0.0 0.255.255.255 eq 138
- permit tcp any 10.0.0.0 0.255.255.255 eq 139
- permit tcp any 10.0.0.0 0.255.255.255 eq 445
- permit tcp any 10.0.0.0 0.255.255.255 eq 2049
- permit tcp any 10.0.0.0 0.255.255.255 eq 20
- permit tcp any 10.0.0.0 0.255.255.255 eq 21
- permit udp any 192.168.0.0 0.0.255.255 eq 137
- permit udp any 192.168.0.0 0.0.255.255 eq 138
- permit udp any 192.168.0.0 0.0.255.255 eq 139
- permit udp any 192.168.0.0 0.0.255.255 eq 445
- permit udp any 192.168.0.0 0.0.255.255 eq 2049
- permit udp any 192.168.0.0 0.0.255.255 eq 20

- permit udp any 192.168.0.0 0.0.255.255 eq 21
- permit udp any 172.16.0.0 0.15.255.255 eq 137
- permit udp any 172.16.0.0 0.15.255.255 eq 138
- permit udp any 172.16.0.0 0.15.255.255 eq 139
- permit udp any 172.16.0.0 0.15.255.255 eq 445
- permit udp any 172.16.0.0 0.15.255.255 eq 2049
- permit udp any 172.16.0.0 0.15.255.255 eq 20
- permit udp any 172.16.0.0 0.15.255.255 eq 21
- permit udp any 10.0.0.0 0.255.255.255 eq 137
- permit udp any 10.0.0.0 0.255.255.255 eq 138
- permit udp any 10.0.0.0 0.255.255.255 eq 139 permit udp any 10.0.0.0 0.255.255.255 eq 445 permit udp any 10.0.0.0 0.255.255.255 eq 2049 permit udp any 10.0.0.0 0.255.255.255 eq 20 permit udp any 10.0.0.0 0.255.255.255 eq 21 deny tcp any any eq 80 deny tcp any any eq 443 deny tcp any any eq 137 deny tcp any any eq 138 deny tcp any any eq 139 deny tcp any any eq 2049 deny tcp any any eq 2049
 - deny udp any any eq 138

deny tcp any any eq 21 deny udp any any eq 137

- deny udp any any eq 139
- deny udp any any eq 445
- deny udp any any eq 2049
- deny udp any any eq 20
- deny udp any any eq 21

permit ip any any

Authorization Policy rule

 asimilyAcl1 EQUALS Block_External_Browsing_ And_External_NFS

07 Contact

For further details, please contact info@asimily.com

Document change control:

# Endpoint Custom Attributes (case sensitive)							
1 Nov 2019	v1, initial revision of document						
11 Dec 2020	v2, Updated steps for various use cases with additional screenshots						

Mitigate Medical Device Cyber Risk with Asimily

Targeted segmentation and device configuration changes rely on a programmatic approach to identifying attack vectors. That's where Asimily comes in—it automates the exploit analysis process, identifying which devices are vulnerable to each MITRE ATT&CK exploit vector, determining the simplest remediation, and verifying it's appropriate for each device (i.e., it won't have clinical consequences).

By combining machine analysis of MDS2 information with profiling data from millions of IoMT devices, Asimily enables customers to make informed decisions about device risk remediation.



Asimily's Risk Management platform:

- creates a complete IoMT inventory, collecting 100+ attributes for each device;
- identifies and prioritizes vulnerabilities;
- recommends clinically validated mitigation actions;
- conducts a full flow analysis for each device, recording all communication patterns across the network;
- calculates risk for every medical device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on healthcare operations;
- enerates ACLs for targeted segmentation and applies them across the network via a NAC;
- flags anomalous device behavior based on profiling data from millions of IoMT devices;
- makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- automates packet capture for forensic analysis of any IoMT device to support root cause analysis;
- supports pre-procurement assessments with comprehensive risk reports for any IoMT device; and
- documents when the device is being used or when the data is being processed by the device so users can understand utilization and operational efficiency.

Asimily can help any healthcare provider drastically reduce medical device cyber risk while minimizing resource and time costs. To see how Asimily can help your organization, <u>arrange a</u> <u>demo today and a free Pre-procurement Risk</u> <u>Assessment for one model of your choice.</u>

info@asimily.com 1-833-274-6459 Sunnyvale, CA



About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, and pharmaceutical companies in the healthcare industry.