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.**

Deployment Licensing + Cen	tificates + Logg	ng + Maintenance Upgrade Health Checks + Backup & Restore + Admin Access + Settin
Deployment	ŵ .	Deployment Nodes List > ise Edit Node General Settings Profiling Configuration Hostname Ise FQDN ise.internal.asimity.com
		IP Address 192.168.1.11
		Role PRIMARY *
		Policy Service Finable Session Services ()
		Include Node in Node Group None + ()
		Enable Profiling Service (j)
		Enable Threat Centric NAC Service (j)
		Enable SXP Service ()
		Enable Device Admin Service ()
		v pyGrid 7

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.

indentit	y Services Eng	jine Hom	e • Contes	t Visibility	Operation	ns I	Policy	- Administration	. → v	Vork Centers
 System 	 Identity Manag 	ement • Netv	ork Resources	Devic	e Portal Manag	ement	pxGrid Ser	vices Feed	Service	Threat 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 Ho	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	Asimity
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 0
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:	🚯 example: pxgrid2.lse.internel.com:8010 or 192.168.1.11:8010	
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	Evienal (
▶ Settings	Inactive account never disabled
	* Password
	* Re-Enter Password
	Generate Password
	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

dentity Services Engine	Home + Context Visibility + Operations + Policy	Administration Work Centers
System Identity Management	Network Resources	vices + Feed Service + Threat Centric NAC
 Identities Groups External Identity 	Sources Identity Source Sequences . Settings	
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 -
	asimilyAcl 1	String - O

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.

dentity Services Engine	Home Context Visibility Operations Policy	Administration Work Centers
System Identity Management	Network Resources + Device Portal Management pxGrid Se	ervices + Feed Service + Threat Centric NAC
Identities Groups External Identit	y Sources Identity Source Sequences - Settings	
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 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.

System Identity Management	Network Resources Device Portal Management ovGrid S	Services Feed Service Threat Centric NAC
Hantitian Groups External Mantit		
Contracts Groups External Mental	y sources wently source sequences - sealings	
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 -

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 - Aviaily_Molical_Device			
	Prefiler Policy *Narw Policy Enabled *Minimum Certainty Factor *Exception Action *Network Boan (MMAP) Action Create an Identity Group for the policy *Parent Policy *Associated CoA Type Bystem Type	Asimily_Medical_Devices 10 NONE NONE No, use existing idently G NONE Cablal Semage Administrator Created	Description (Valid Range 1 to 65535)	
	Ruies If Cendian CUSTOMATTRBUTE_	mirtiyDeviceEartiy	Conditions Details CONTAINS Molical Devices CONTAINS Molical Devices	<u></u>

Figure 16: Profiling Policy – Asimily Medical Devices

willian	Profiler Policy List - Avialty Motiv	d Devices		
	Profiler Policy			
- E -		Name [Asimily_Medical_Devi	ices Description	
Profiling Policies	Policy Er	abled 🗾		A
Logical Profiles	* Minimum Carlainty	Factor 10	(Valid Range 1 to 65535)	
	* Exception	Action NONE	*	
	* National Scan (MMAP).	Addres NONE		
	Create an identify Group for the	policy () Yes, create matchin	a identity Group	
		O No, use existing Ide	entity Group hierarchy	
	* Parent	Policy NONE	-	
	* Associated Co.	Tape Citybal Settings	-	
	Byster	Type Administrator Created		
	Rules		Conditions Details 2	
	If Condition CUSTOMATTR	BUTE animilyDeviceFamily	CUSTOMATTRIBUTE asimily Deviced analy	
			CONTAINS Medical Devices	
	Save. Renet			k.

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.

durb Identity Services Engine	Home + Context Visibility + Operations	Policy Administration Work Cent	819	
Policy Sets Prolling Posture C	iant Provisioning + Policy Elements			
Profiling	Profiling Policies			
	A			
(2) * 臣 *	1 - / ER +AN DUDION XD	dete + gelinort gelinort +		
Profiling Policies	Profiling Policy Name	 Policy Enabled 	System Type	Description
* 🧱 Lagical Profiles	2Wire-Device	Enabled	Caco Provided	Policy for 2thre-Device
	C 3Com-Device	Enabled	Caco Provided	Policy for 3Com-Device
	Asstra-Device	Enabled	Cisco Provided	Policy for Aastra-Device
	Asstra-IP-Phone	Enabled	Caco Provided	Policy for Aastra-IP-Phone
	Aarohave-Accesse-Point	Enabled	Caco Provided	Policy for Aerohow-Access-Poett
	Aarohive-Device	Enabled	Caco Provided	Policy for Aerohive-Device
	American-Power-Conversion-De	wice Enabled	Cisco Provided	Policy for American-Power-Conversio
	Android	Enabled	Caco Provided	Policy for all Android SmartPhones
	Android-Amazon	Enabled	Caco Provided	Policy for Android Amazon
	Android-Amazon-Kindle	Enabled	Caco Provided	Policy for Android-Amszon-Kindle
	Android-Amazon-Phone	Enabled	Caco Provided	Policy for Android Amston Phone
	Android-Amazon-TV	Enabled	Cisco Provided	Policy for Android Amezon TV
	Android-Asus	Enabled	Ceco Provided	Palcy for Andraid-Asus
	Android-Google	Enabled	Cisco Provided	Policy for Android-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	trol Reports
Policy List Endpoint Assig	Inment			
List > New Input fields marked with an name *	asterisk (*) are require ANC_Quarantine	ed,		
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						01	
Party Sets + Defeat	Library		Editor					CHARLENNED COLD 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						
 Automatic Prop - Local Encloses (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
See an or a	C 64P.7L3							10 A111
2 0. min	G Overst, Ploy	ø						
	MAC, IN, SAM	0						
 Americano Weights 	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_1018							
							Chief Use	
		_		_				

Figure 21: ANC Quarantine Authorization Policy – 1

time stanty Services Engine Har	a + Constituting + Operation + Pathy + Administration + West Consti	😸 Litter Managar 🛝 🕸	
Policylan Policy Dokes Cherol	Producenceg + Proby Elements		
Policy Sets + Default		Result/8 milliounits Print	time
Status Policy Set Name	Description Conditions	Allowed Protocols / Server Sequence	# 1925
Seats			
@ Setut	Subjuit parky set	Default formuld, Autors + =	1
Authentication Policy (3)			
> Authorization Policy - Local Exception	ris [1]		
♥ Authorization Policy - Global Escripti	ens (0)		
		Persuits	
Sistus Rule Name	Conditions	Profilm Security Groups Hits	Actions
Search			
/ @ Quantum	E Instan AnDholog RQUARE Querantive	(chernen) 🔹 Quantine Jyden + 💌	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 Configurat	ion Reports Bookmarka		ព	4	atmin ~
Haemodynam	<pre></pre>	Annet Details Topology Vulnessabilities = MDS2 Impor	a Anomaly Recall Utilization	Flow Analysis		
i		Recommendations Application/Device Bosuity Posts	e + MD62		DEVICE	EXPOSURE 9
		Q South Resulting Astronomy		🔳 Include Fixed	Vew High R	New AS
<i>,</i> =		Recommendations	No. OF High Risk CVES	Action		
GE Healthcare Mar	o-Lab	Stop Browsing non-whitelet domains using internet explorer SII you patch internet explorer or SII you set internet security mean to total DB HII you diables where excitation and write X		2m		
Device Params		scentrals				
OUI Manufacturer	Hewlett Packard	Size and benefits provabilities (service and using				
Serial Number		network file share estemaily And using email fill you patch		₽ m		
Software Version						
Facility	Facility1	Stop using Microsoft Edge till you patch or Stop Browsing		4.00		
Department		external websites using Microsoft Edge		210		
Location		Stop web browsing non-whitelisted domains until you patch				
Sub-Modules			•	×14		
Hardware Architecture		Disc using Microsoft Word till you patch	5	26		
Stoles (PH)	-					
Transmits of H	-	Stop using Microsoft Edge or Internet Explorer till you patch				
CMEMS Id		er begi browning branner webaltes using Microsoft Edge or Internet Esplorer		100		
IT Parame		Read the formation of the last and the first section in the sector				
P Address	1020213.119	Frewall		Arts		
STREET, STREET	(D+C2)					

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.



ASIMILY					n 🕐 atrin 🗸
	CVE-2013-3123				
		Improper Restriction of Operations with	thin the Bounds of a Memory Buller (2.11)		
		Microsoft Internet Explorer & Brough 2 orafted web site, sike "Internet Explore	10 allows remote attackers to execute arbitrary code or cause a denial of se or Memory Comuption Vulnerability.* a different suinerability than CVC-2013-	vice (namory comption) via a 9111.	
	Device Configuration Trigger:	Device being used for web browsing u	aling Internet sopkow		
	Vulnerability Exploit Vector:	Web browsing non-whitelisted domain	is using affected version of internet explorer		
GE Healthcare Mc		- CONFIGURATION Stop Browsing non-writelist domain	ins using internet explorer till you patch internet explorer or till you set i	nternet security cone to high	
		OR III you disable active scripting i	and active X controls		
	OVE PARAMETERS				
	Name	Value	Nere	Value	
	Confidentiality impact	NONE	Confidentiality Multiplication Factor	MEDIUM	
	integrity impact	нан	Integrity Multiplication Factor	MEDERM	
	Availability impact	нан	Availability Wultiplication Factor	HIGH	
	Allack Victor	NETWORK	Attack Complexity	LOW	
	Privilege Required	NONE	User Interaction	NONE	
	Remediation Lawsi	TEMPORARYFO	× -		

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 Su	mmary Configuration	on Reports	Bookmarks					10	a V	0	👤 admin ~
Asset Details	Anomaly Valnorabilit	ies impact Red	al Utilization	Turning Mig	ation							Total Court: 1
Categories 1	low Device View											₽ Action
9	100mm 10 A 20 104 +											
	IP Address	Mac Address	Manufacturer	Device Type	Device Model	05	Fadity	Anomaly Score	mai.	Impact	Likeliho	M
	0 10.4.20.104	00:50:54:95:a4:a2	GE Heelthcare	Imaging Workstation	-	windows_10	Facility_3	۰	•	•	•	
Power 100	•									'	Showing 1 o	at of 1 records.

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

Take Action			(g) atrix -
			Total Court: 1
Osos DE Block External Browsing 83,143			Anton
permit top any 192.168.0.0.0.0.355.255 eq.80 permit top any 192.168.0.0.0.355.255 eq.443 permit top any 192.15.0.0.0.355.255 eq.443 permit top any 172.16.0.0.0.15.255.255 eq.443	Î.		
permit top any 30.0.0.0.0.256.255.255 eq.443			est.
Generale ACI. Downitiaal ACI.			
			nd of 3 meteries

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	esults	
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 8910111 permit top any 192 168.0.0 0.0.255.255 eq 443 931412 permit top any 192 169.0.0 525 255 eq 40	
+ Posture	1617101 permit barry 172.10.00 0.152525256 e 443 9202122 permit barry 10.0.00 0.255255256 e 443	
Client Provisioning	23948202 permit top any 10,000 0 250 250 250 250 eq 443 6272829 deny top any any eq 60 3031323 deny top any any eq 443 334356 permit lip any any 3738394	
	Check DACL Syntax	Ð
	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	Ilent 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
	Common Tasks DACL Name OnlyinternaHttpAccess ACL (Fitter-ID) Security Group VLAN

Figure 28: Create Authorization Profile and associate with DACL

Point of Point CoamProvidement Provider CoamProvidement Provider CoamProvidement Provider		
Status Policy Set Name Description Conditions Allowed Protocols / Server Status Policy Set Name Description Conditions Defcort Protocols / Server Image: Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Condition Server Image: Condition Server Image: Condition Server Image: Condition Server Condition Server Image: Condition Server Image: Condition Server		
Status Polety Set Name Description Conditions Adoved Protocols / Service Image: Service in the service in the service interval i	Reset	Love
Construint Office Office Defice/Interview Defice/In	er Sequenc	e HBS
Optimus Default solution Default solution <thdefault solution<="" th=""></thdefault>		
		110
Autorization Policy - Local Exceptions (1) Autorization Policy - Local Exceptions (1) Conditions Results Results Police Results Police Security Droups GenetitientaPhylocass L EndPoints asimple(1) EQUALS One, Imming, HTTP, Access Security One, Interpreted, HTTP, ACCES Genetitiential Genetitiential		
Assults Results Results <t< td=""><td></td><td></td></t<>		
Status Rule Name Conditions Profiles Becurity Droups Search		
Source Competitional Competitional Competition Competi	Hts	Actors
Onentimatetpacess b Endheins asimbledt Eddalls One, menal HTTP, access		
	. •	٥
Authorization Policy - Global Exceptions		
Authorization Policy (13)		
	Reset	Leve

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 Play Analysi		
-		One Day One Week	Al Time E-	•
GE Healthcare Volu	son E8		MAG	-
Device Params		16412.29		
00 Merufacturer	Advantech Technology (CHINA) Co. Ltd.	TT Workstation	Set.	-
Serial Number		10 101 964	Most recent	-
Software Version			networking device ritr	
Facility	Facility.1	10.20.209.171	Denke with anomaly	
Department		Instant Work station		
Location		b) 18/ 111 19)		
Sub-Modules				
Hardware Architecture				
Stores of 14	-			
Tanania ePie	-			
CMMSIN				
IT Params				
P Address	10.20.209.171			
	(OHCP)			

Figure 30: Device Topology

ASIMILY	Assets Burne	very Configuration	Reports	Bookmarks						а ,	ð 9	🚺 admin ~
Asset Details Asset	wy Watherschilden	Impact Recall	Utilization	Textury Milger								Total Count: 1
Cutagorius View	Device View											Action ■
Q #Atten	55.30.508.171 +											
	tdress	Mac Address	Manufacturer	Device Type	Device Model	05	Facility	Anomaly Score	Rek	Impact	Likelhoo	•
		02.00 ab:14.38 cc	GE Healthcare	Ultrasound	Volusion EB	windows	Facility,1					
Rows 100 -											Showing 1	out 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
	Device View											Co Back
E Oltra	isound											
		10.20.209.171						00:0kub/94-38:cs				
		GE Healthcare						Ultracond				
	Device Model :	Volueon EB						windows				
	Facility :	Pacify_1										
_												Action
Q Territ												
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 Barra	ary Configuration	Take Action			×	n A	0	() atom ~
				•	Book External Revening 🔹				
E Ultra									
			Generate ACL						

Figure 33: Device Topology View – Take Action

ASIMILY		Take Action					(g) admin v
				Restrict Neighbor Traffic			
Q Utras		permit udp any a permit udp any a permit up any hos permit ip any hos deny ip any 192. deny ip any 172.	ny eq 68 ny eq 53 r 10.363.111.190 r 10.363.96.4 166.0.0.0.255.255 18.0.0.0.15.255.255		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	Bookmarka		R	۵	0	1 admin v
Asset Details Anons	vy Winesbillies Impact Recal Utilization	Tepology Miligation					Total Court: 65
Categories View [Invice View						Actor
Q Search Per							
	Device Type		Number Of Devices				
	Inflation pump		4508				
	IT Workstation		1086				
	Medical Device		13				
	Cull Station		555				
	Vital Signs Monitor		805				
	Utresound		258				
	Central Manitoring Station		194				

Figure 35: Mitigation – Category View

then identity Services Engine	Hanne + Canted Vestaldy + Operations + Policy + Administration + Walk Centers	Lumes Wannes 📥 🤨 🔍 🔍 🔍
PolicySets Profiling Posture	e DestPosisioning +Polo Benerits	
Dictionaries + Conditions	Reads	
	Authorization Profiles > Inve Authorization Profile	
· Additional and	Authorization Profile	
* Authorization	"Hame Infusor_Pumpi	
Authorization Profiles	Description MAB for IMARIO Pumps	
Downloadable ACLs	*Access Type ACCESS_ACCEPT +	
+ Profiling	Network Device Profile 👔 Claca 🔹 🕀	
+ Postare	Denico Template	
+ Cliest Provisioning	Track Rowmann E D	
	Passade (density mechanic D)	
	* Common Tasks	
	Z EACL RIPHO PERMIT_ALL_TRAFTIC O	
	E va	
	C Decurs Group	
	Z VLAN Tag D 1 (888, Tag) DAtama (201	*
	Advanced Attributes Settings	
4	a	

Figure 36: Create Authorization Profile – Assign VLAN ID

deals identity Services Engine Home	+ Context Visibility + Operations	+Policy +Administration	+ Work Centers		License Warning 📥 🔍	
Policy Sets Profiling Posture Client Provi	sioning + Policy Elements					
Status Policy Set Name	Description (Conditions			Allowed Protocols / Server	Sequence Hits
Dearch						
@ Debuilt	Default policy set				Default Network Access	** + 941
Authentication Policy (3)						
♥ Authorization Policy - Local Exceptions (1	ŋ					
				Results		
* Status Rule Name	Conditions			Profiles	Security Groups	Hts Actors
Search						
Infusion Partips VLAN	b EndPoints asimit/Device?)	pa EQUALS Infusion pump		(+Influsion_Pumps)	Selection tal	• •
Authorization Policy - Global Exceptions						
Authorization Policy (13)						
						Reset Save

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

ASIMILY	Y Assets Su	rmmary Configurat	ion Reports	Bookmarks						β	0 🚺 admin ~
Asset Details	Anomaly Valuendal	lies impact Pla	cal Ultration	Tarity M	ption						Total Court: M
Catagorias	View Device View										PAdes
Q 🖬	vice Family : Imaging Device	e > OS : windows >									
	P Address	War Address	Manufacturer	Device Type	Device Model	05	Pacility	Anomaly Score	Rak	Impact	Likelhood
	•10.24.195.178	ec613/73H04/8	GE Healthcare	imaging Workstation	Xdets	windows	Facility.1				
	• 10.24 195 173		PLUPILM Corporation	XiRay		windows	Facility_1				
	●10.28.116.64	34/02/05/w15e-44	FILIFILM Corporation	Digital Radiography		windows	Facility.1				
	●10.24.116.171		FULIFILM Corporation	xitay		windows	Facility,1				
	●10.28.116.28	00.43.93.99.54.38	GE Healthcare	Ultrasound	LOGIQe	windows	Facility.1				
	• 10.24.202.32	M35349e1775	Del Inc.	imaging Workstation	847	windows	Facility_1	•	3	•	•

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 139 deny tcp any any eq 139 deny tcp any any eq 2049 deny tcp any any eq 200 deny tcp any any eq 20 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 445

deny tcp any any eq 21 deny udp any any eq 137 deny udp any any eq 138 deny udp any any eq 139

- 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.