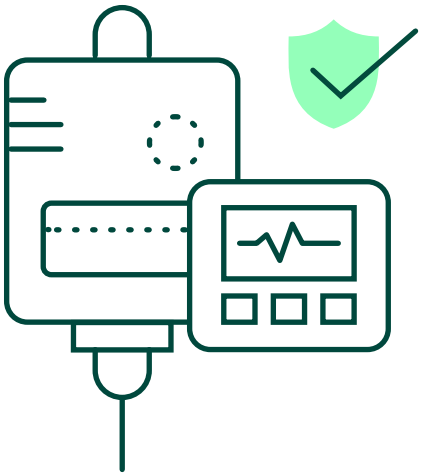
Asimily Insight Cisco ISE Integration Guide

Integration details
and use cases

asimily

Contents



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

IDENTIFY Identify device parameters, applications, and network parameters. Perform deep packet inspection of customer's data, and understand asset utilization and usage.

PROTECT Protect the resources by applying network controls and organizational policies to block, segment, and isolate suspect devices.

DETECT Detect vulnerabilities and anomalies (against the baseline). Prioritize high likelihood, high impact devices for vulnerability management and provide workarounds to mitigate the risks.

RESPOND Respond to specific threats and take actions based on findings. Perform forensic analysis to investigate the root cause of identified problems; assess data flows, protocols used, and data Tx/Rx. Capture network traffic from devices behaving abnormally and save it for offline analysis.

RECOVER Recover through plans created via device profiling: unique device characteristics are captured and defined; utilizing data analytics to profile unique behaviors, configurations, and controls.

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.

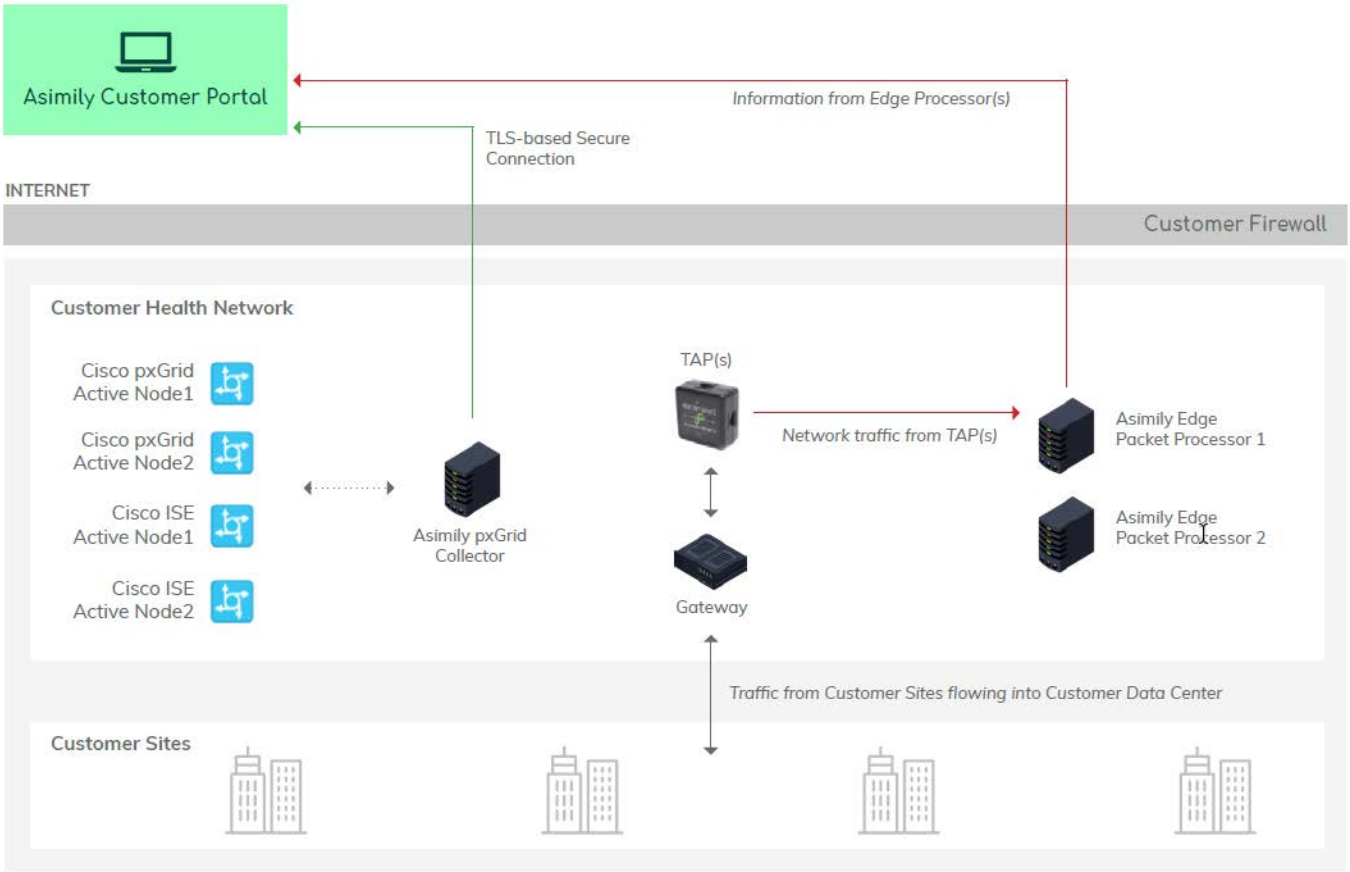
02 On-premises Asimily deployment: In an on-premises deployment the collector runs within one of the Asimily on-prem servers and there is no need for deploying a dedicated Collector.

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.

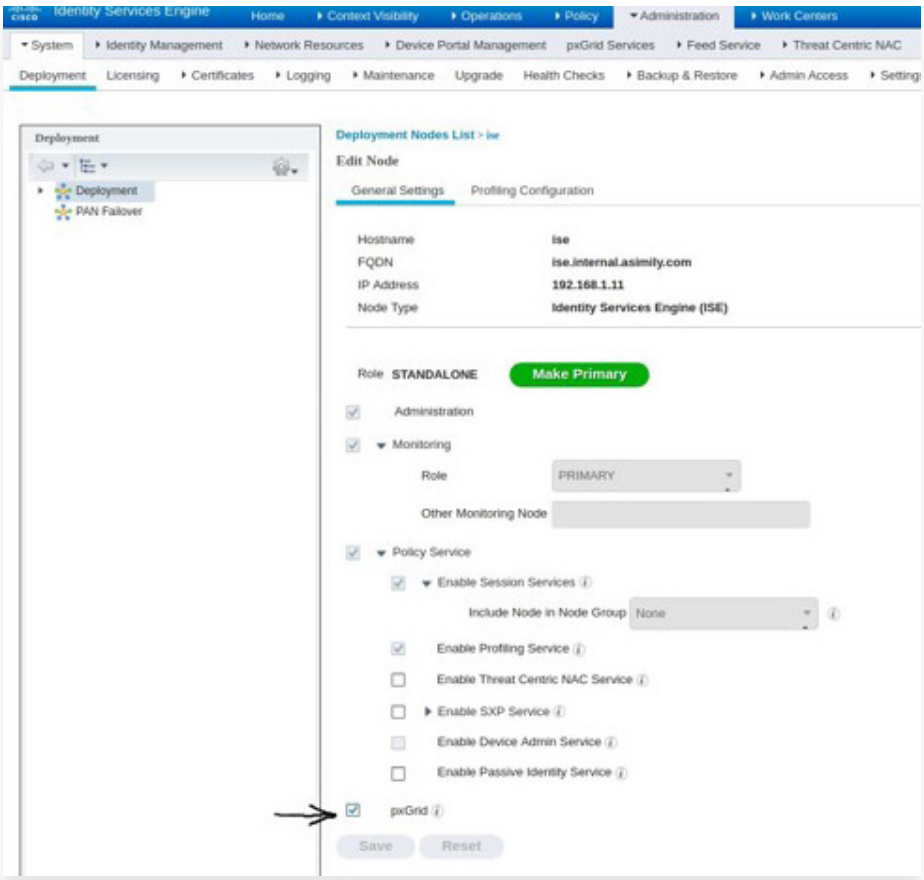
06 Depending on the use cases detailed in Section 5, there would be a combination of actions within the Asimily portal and Cisco ISE portal that are detailed in that section.

04 Asimily Insight and Cisco ISE Configuration

a. Enable pxGrid Services within Cisco ISE

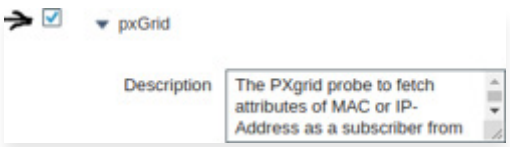
STEP 1

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



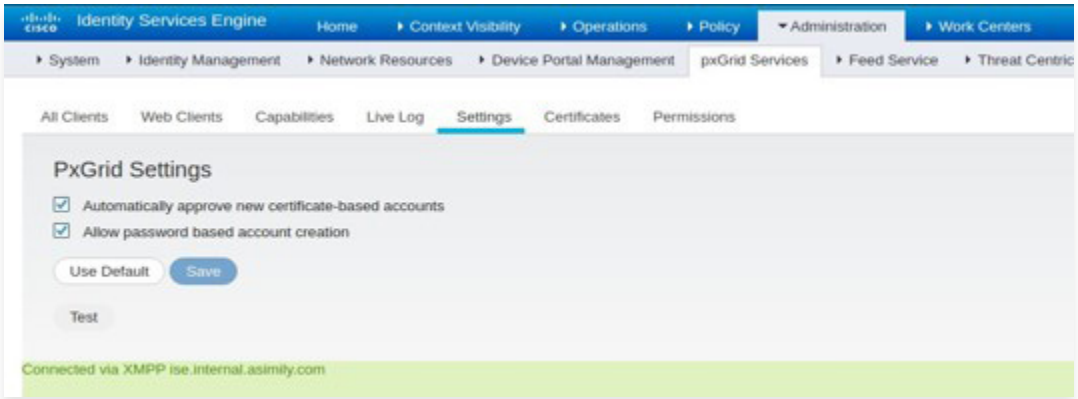
STEP 2

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



STEP 3

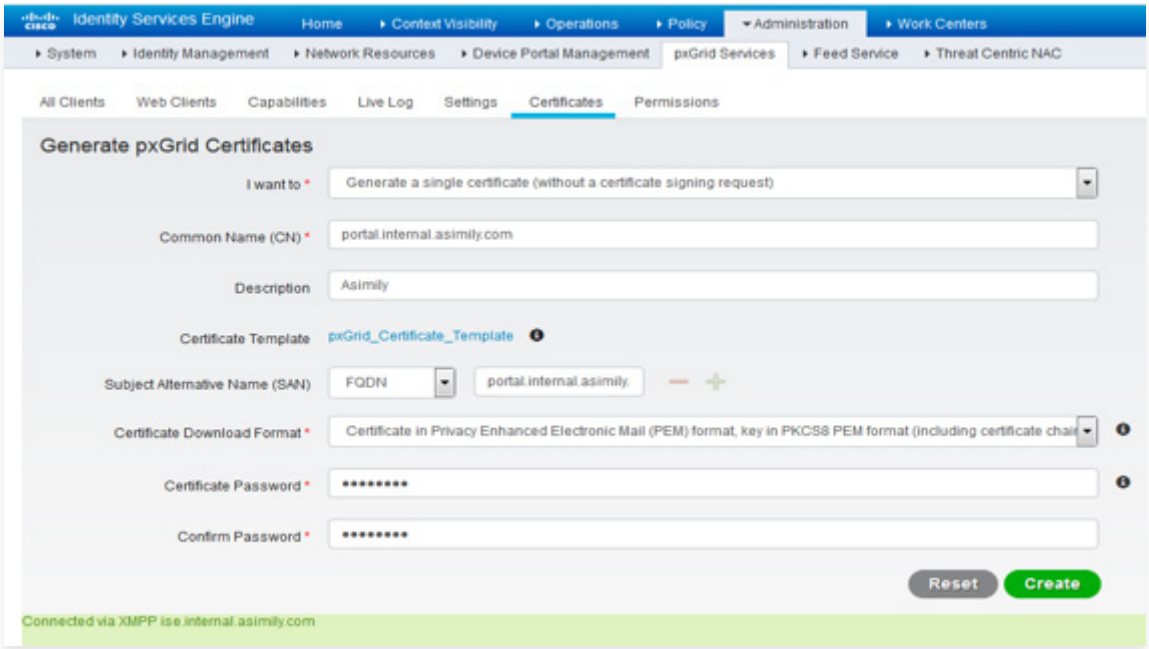
Configure ISE to approve all pxGrid Certificate-Based Accounts: Navigate to **Administration > pxGrid Services > Settings,** and check both boxes show in the figure below.



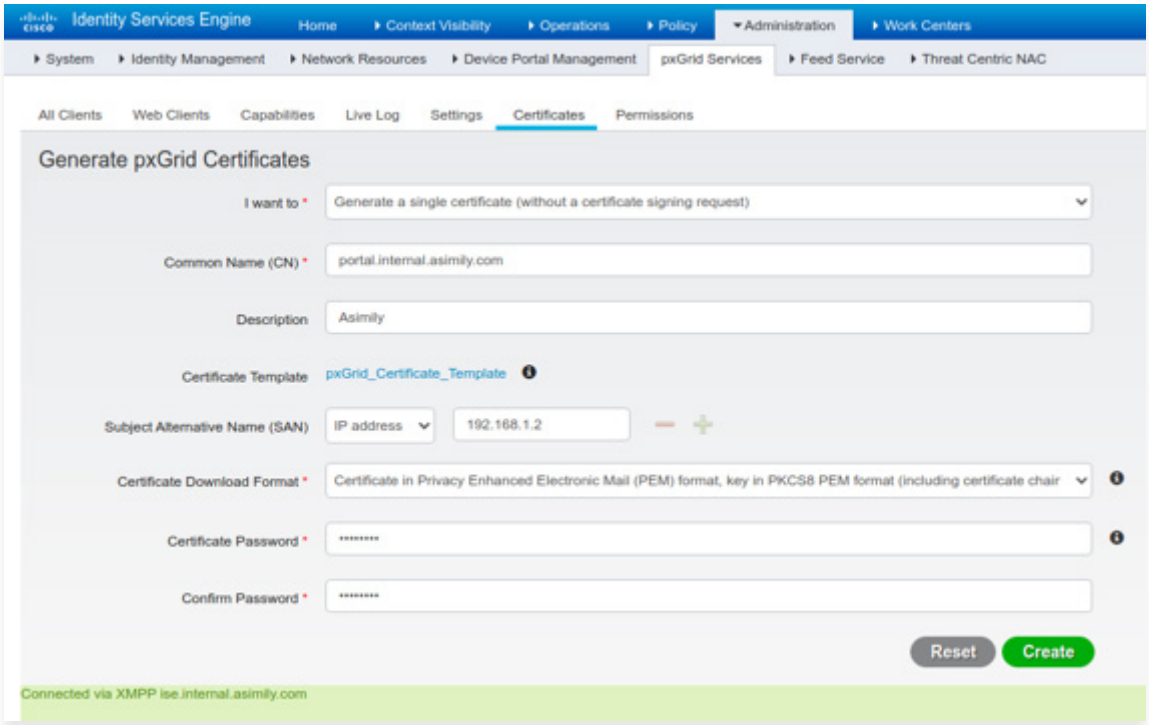
b. Generate pxGrid certificates for cert-based authentication

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

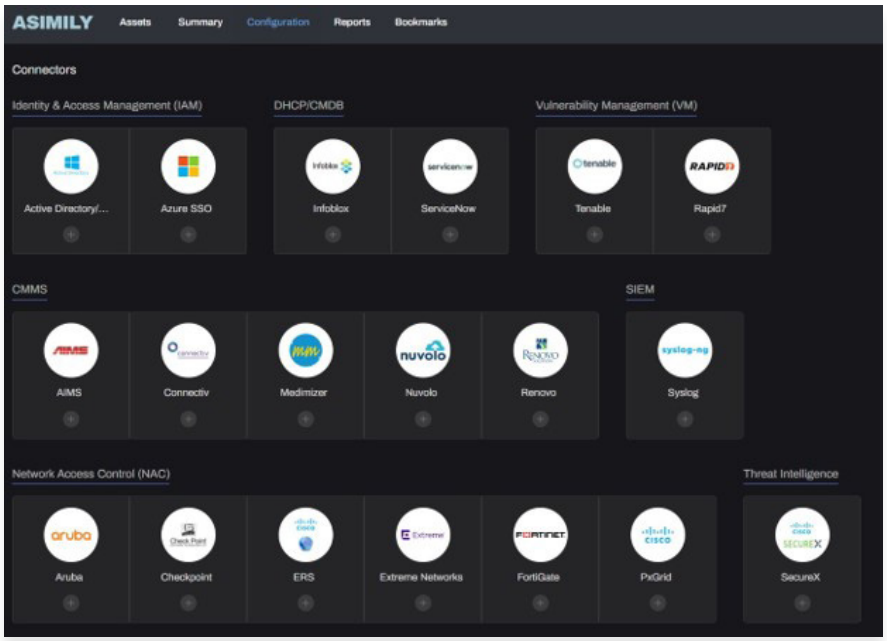


b) Subject Alternative Name (SAN) as IP Address



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:

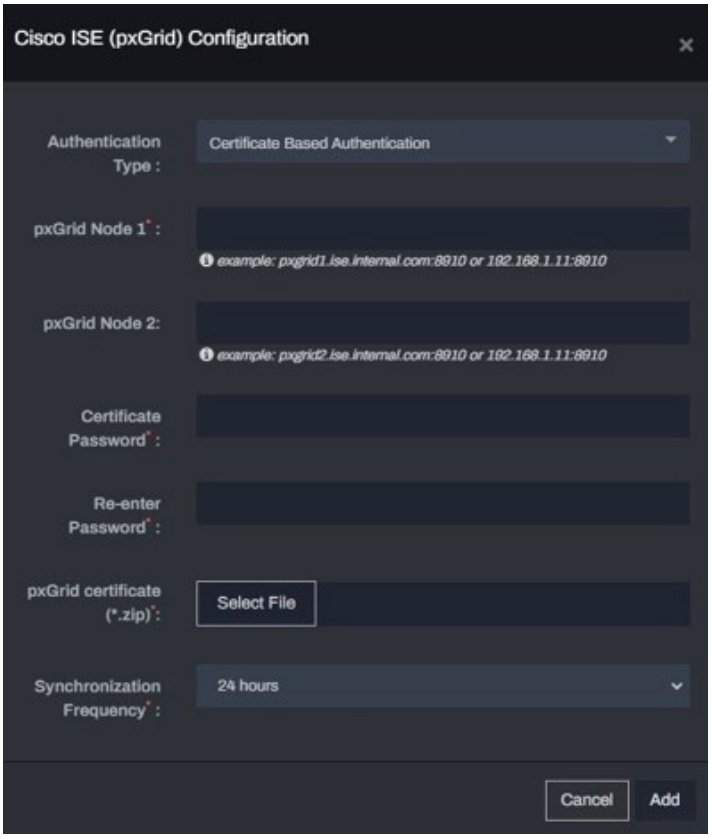
01 pxGrid Node 1* (required): Example: pxgrid1.ise.internal.com:8910 or 192.168.1.11:8910

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.

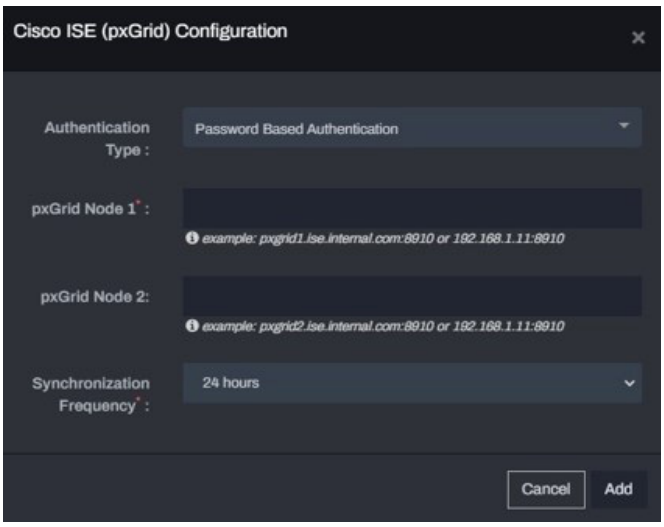


ii. Password Based Authentication:t

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



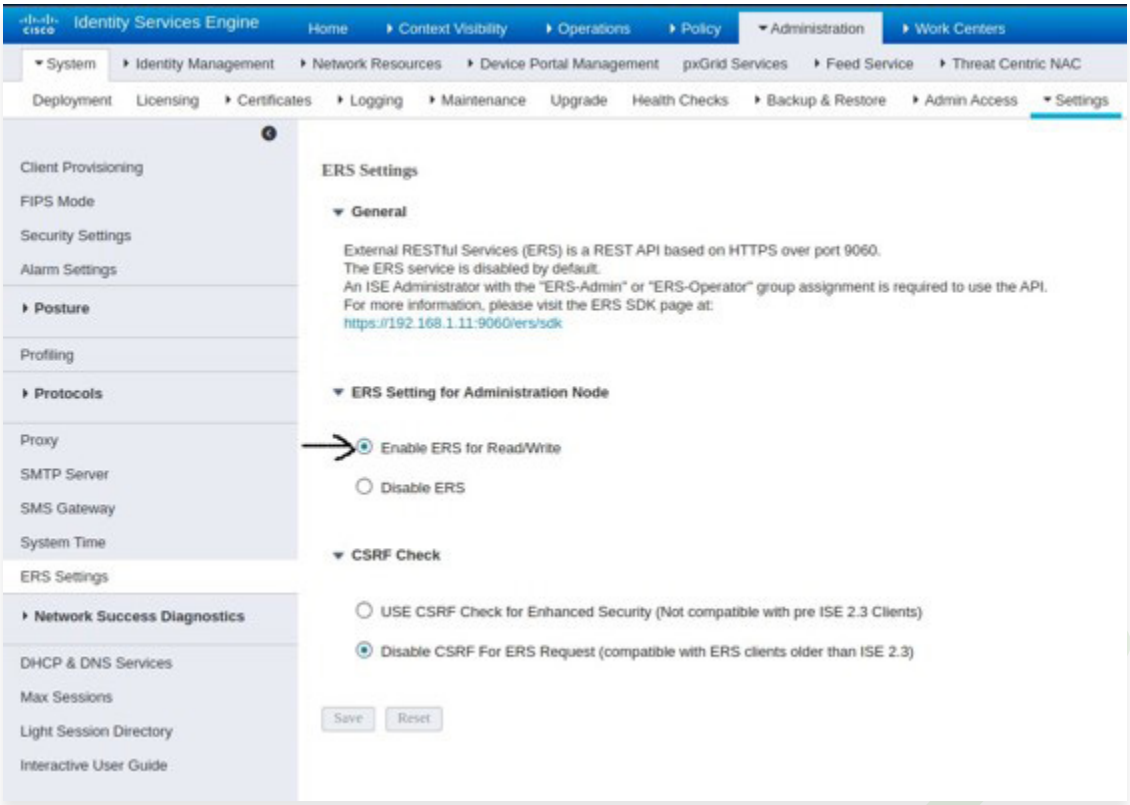
d. Enable ERS API within ISE

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#pgfId-1079726

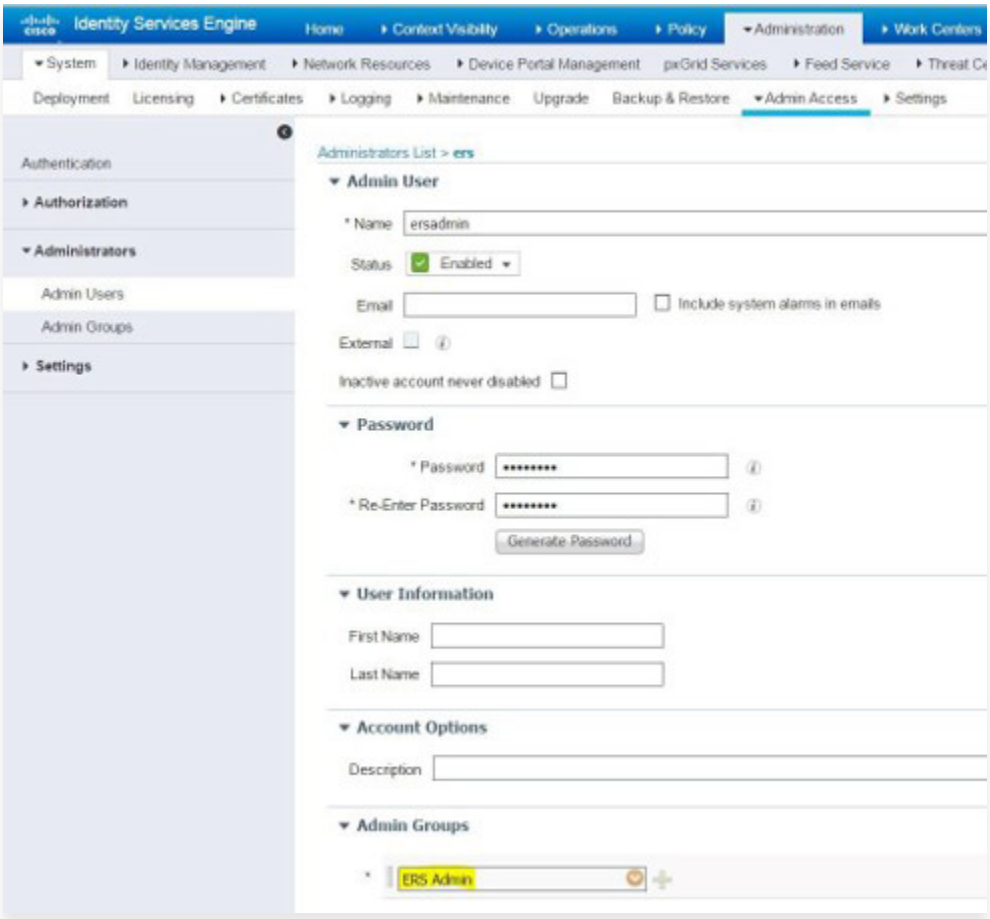
STEP 1

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.



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)

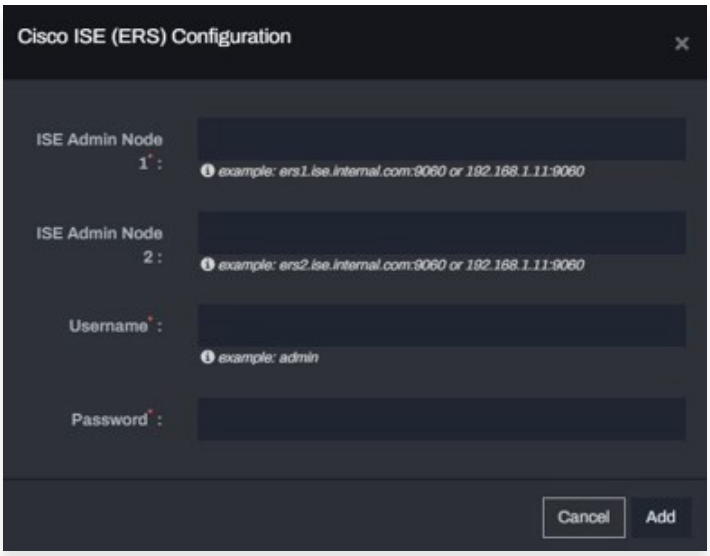


Figure 12: Asimily ISE ERS Configuration

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

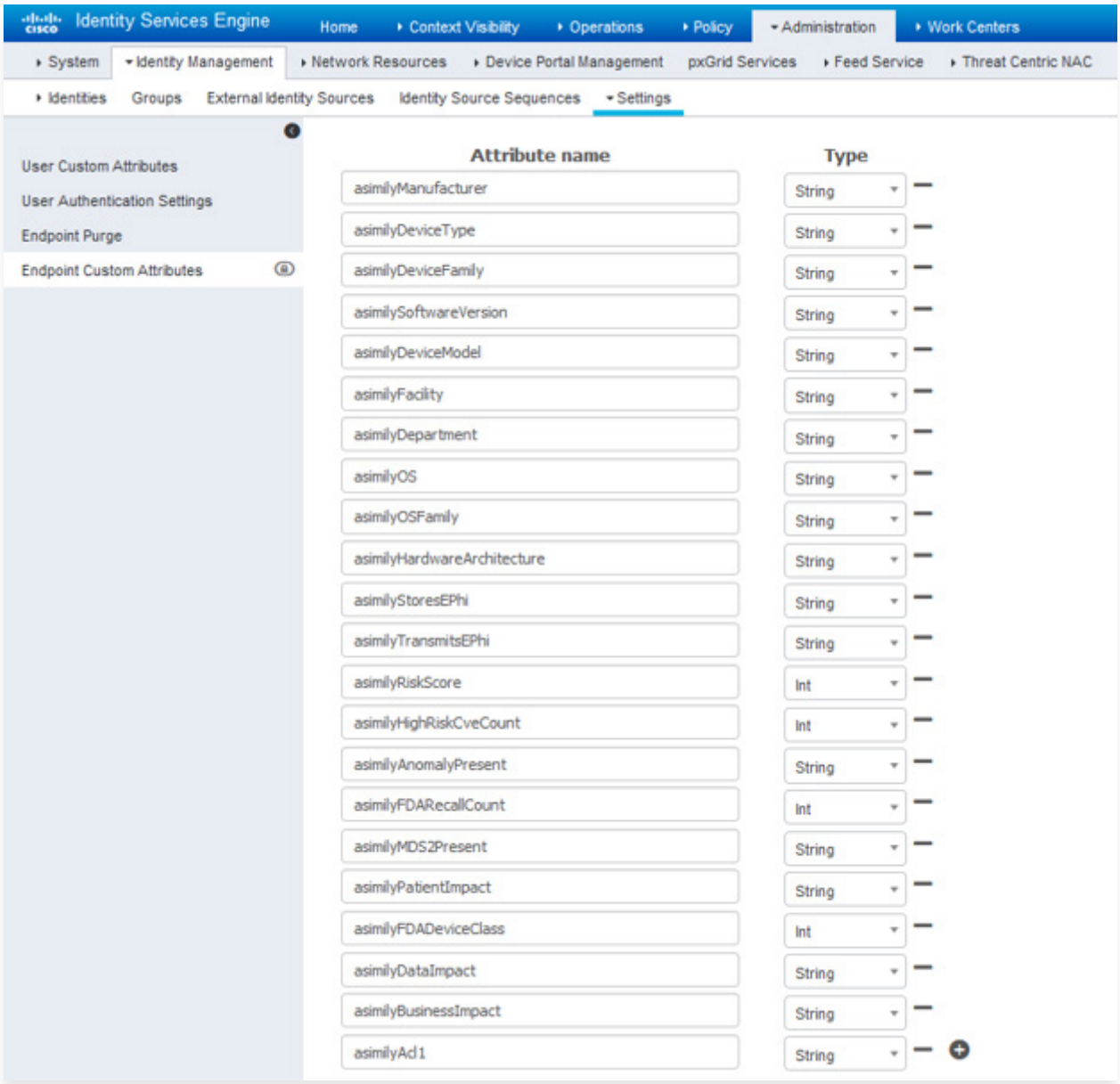


Figure 13: Define Custom Attributes within ISE

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

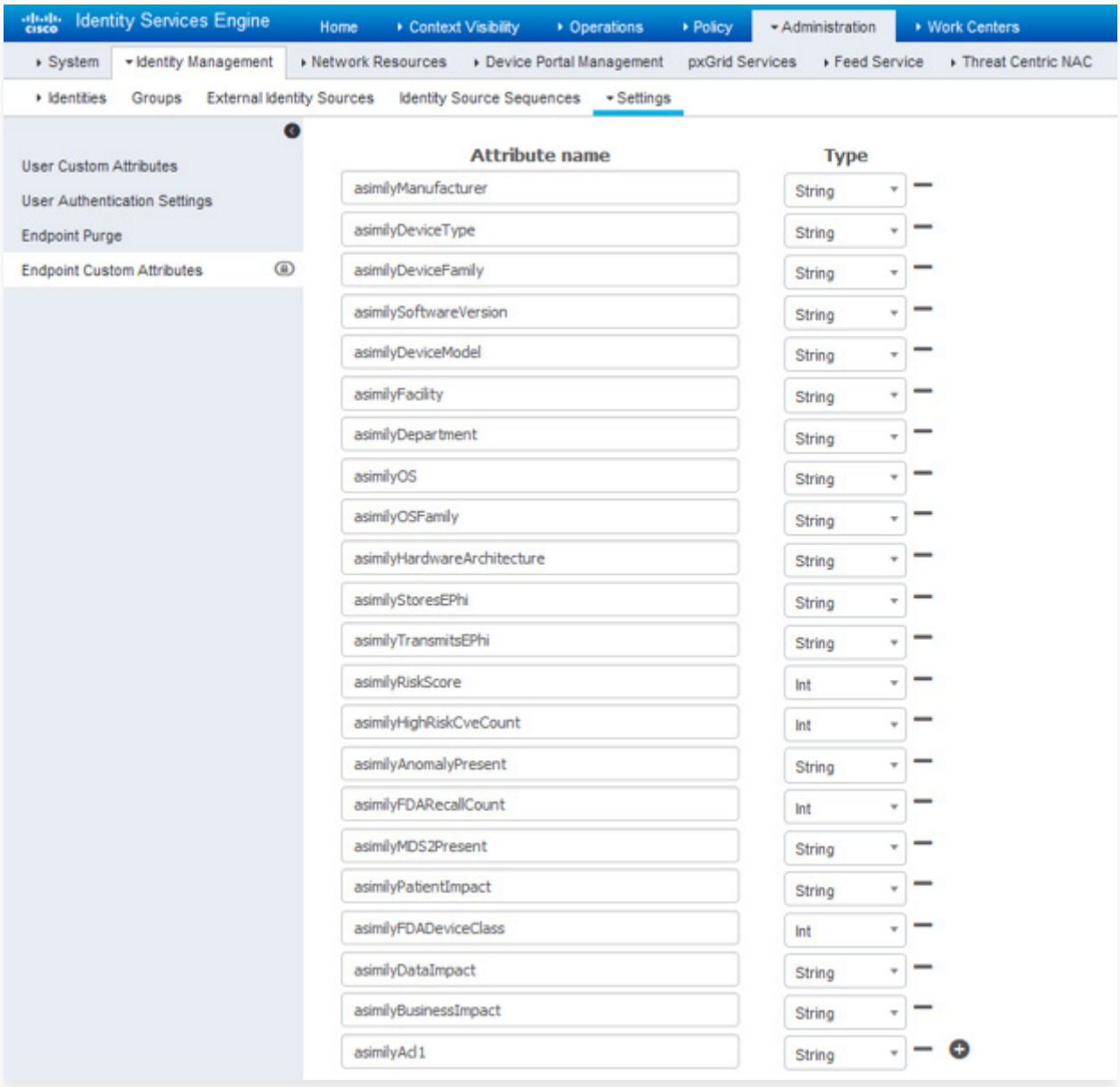


Figure 14: Figure 14: Asimily Device Parameters – Context-In Functionality

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.

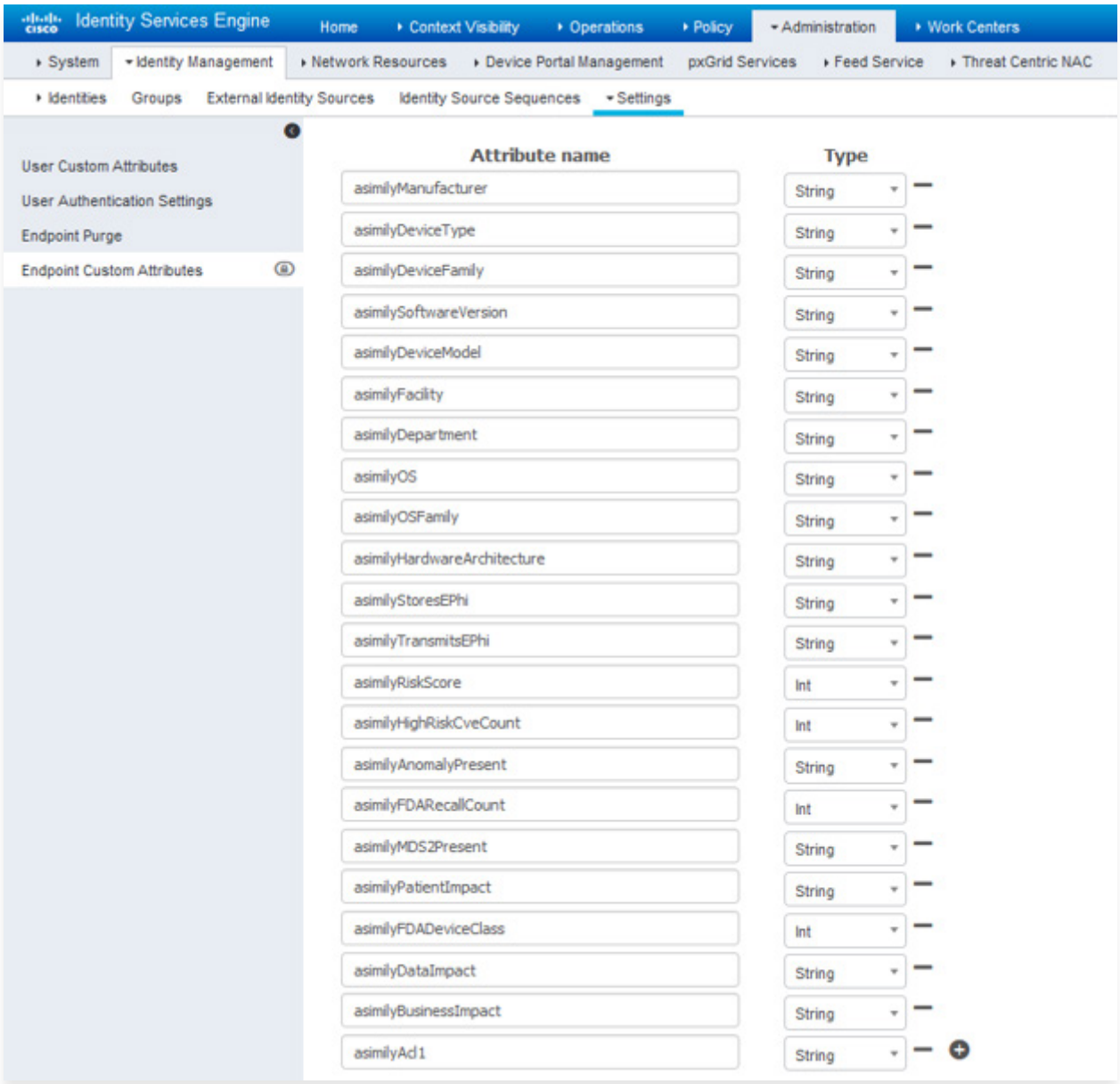


Figure 15: Cisco ISE Device Parameters

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.

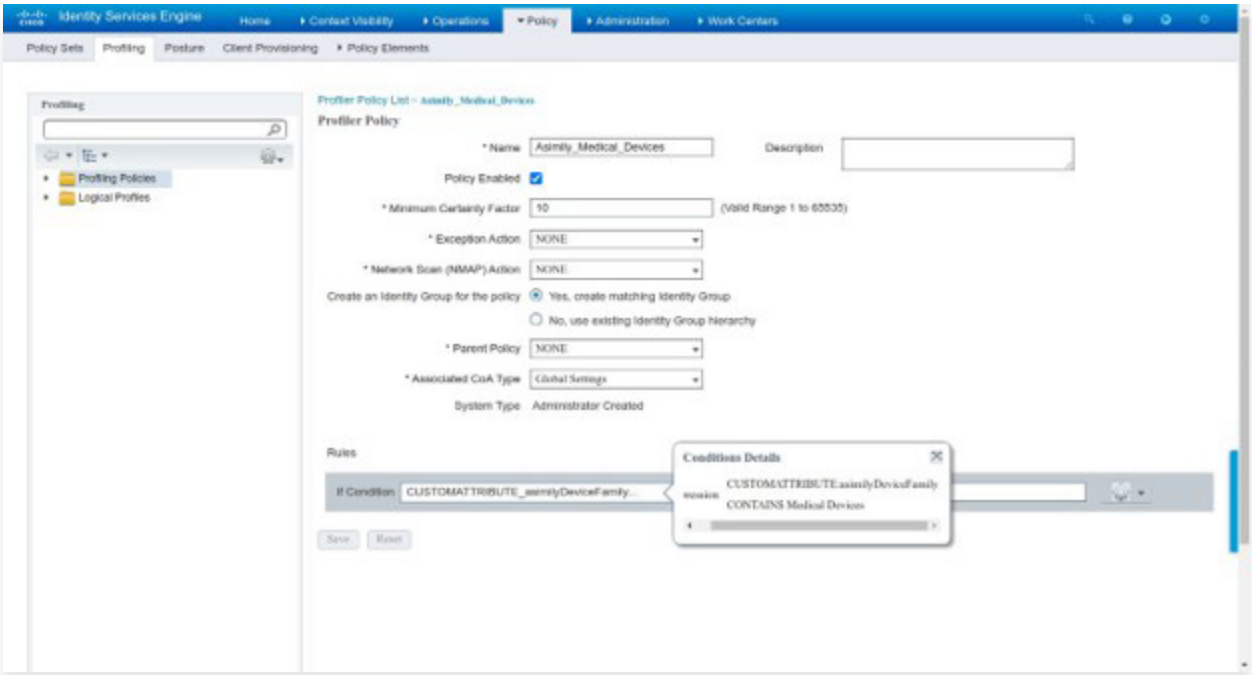


Figure 16: Profiling Policy – Asimily Medical Devices

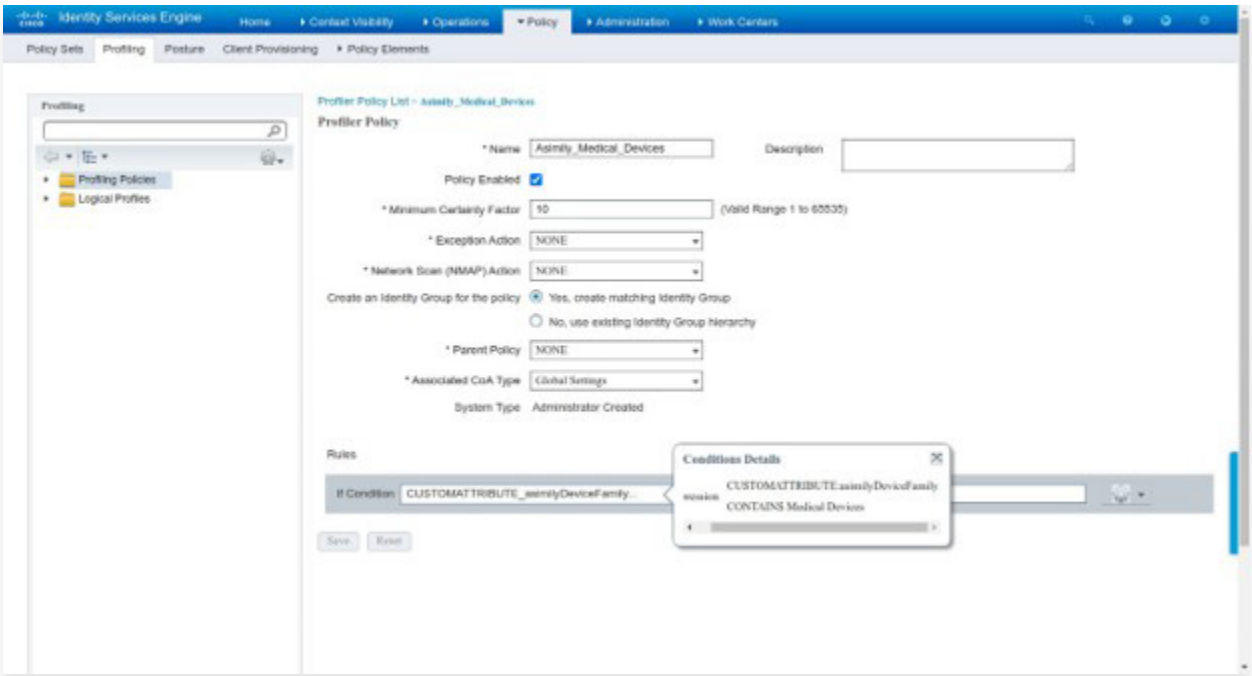


Figure 17: Profiling Policy – Asimily IoT Devices

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.

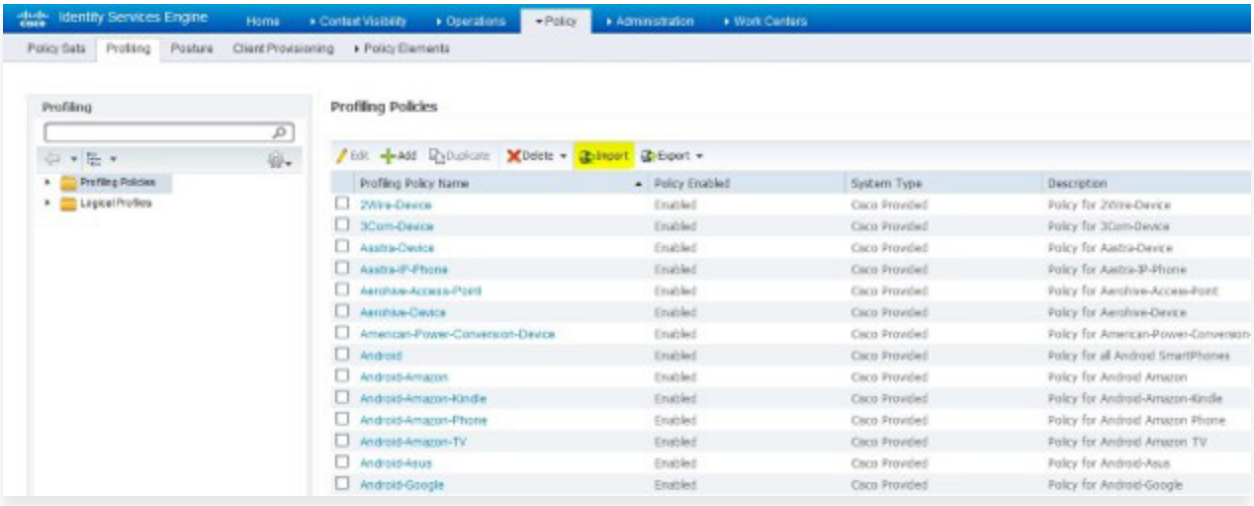


Figure 18: Import Profiling Policies

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

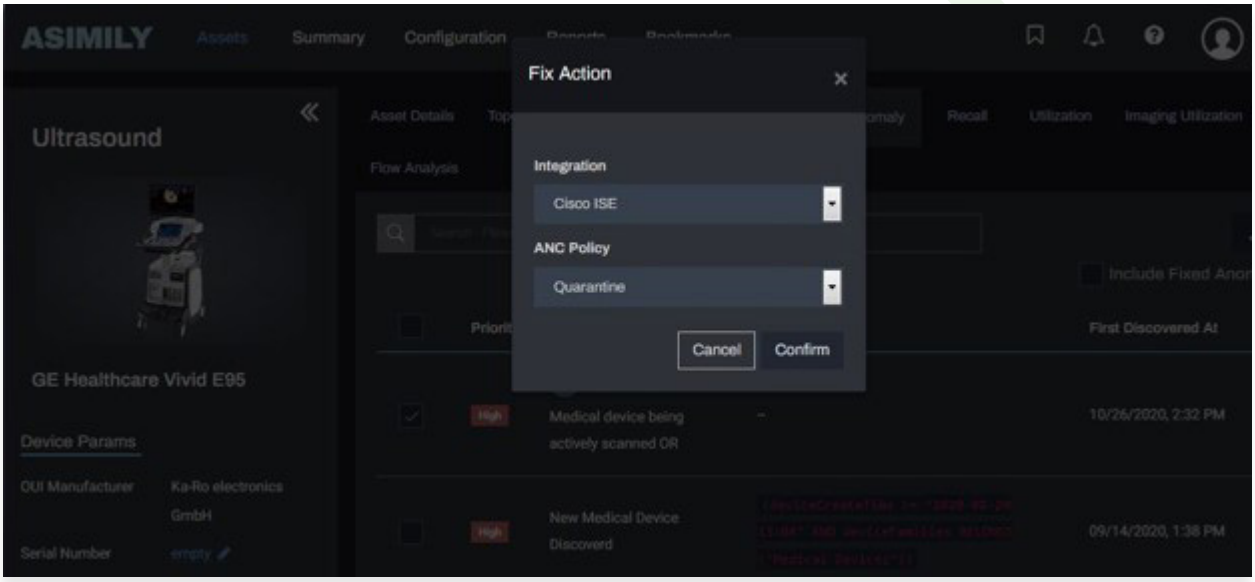


Figure 19: : Import Profiling Policies

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.

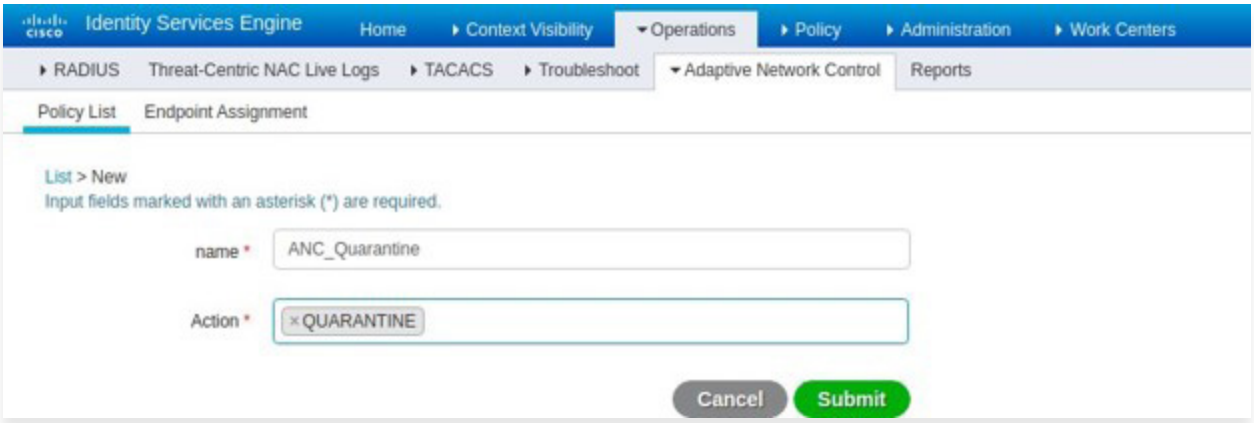


Figure 20: ANC Quarantine Policy Creation

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.

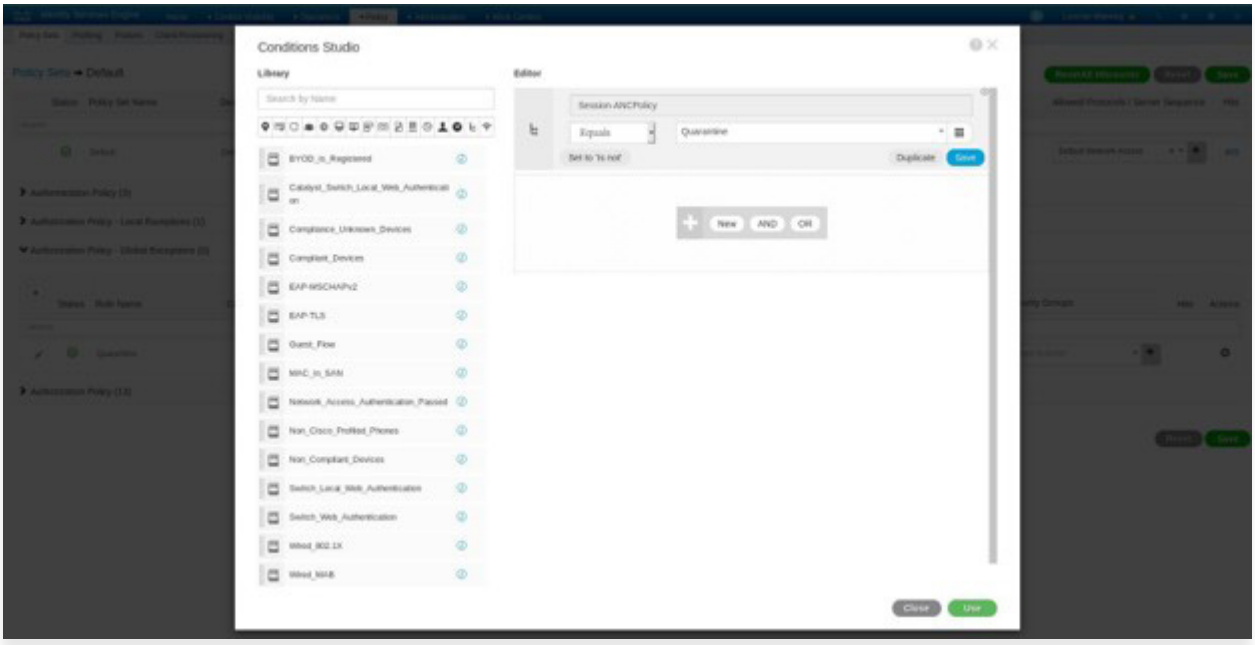


Figure 21: ANC Quarantine Authorization Policy – 1

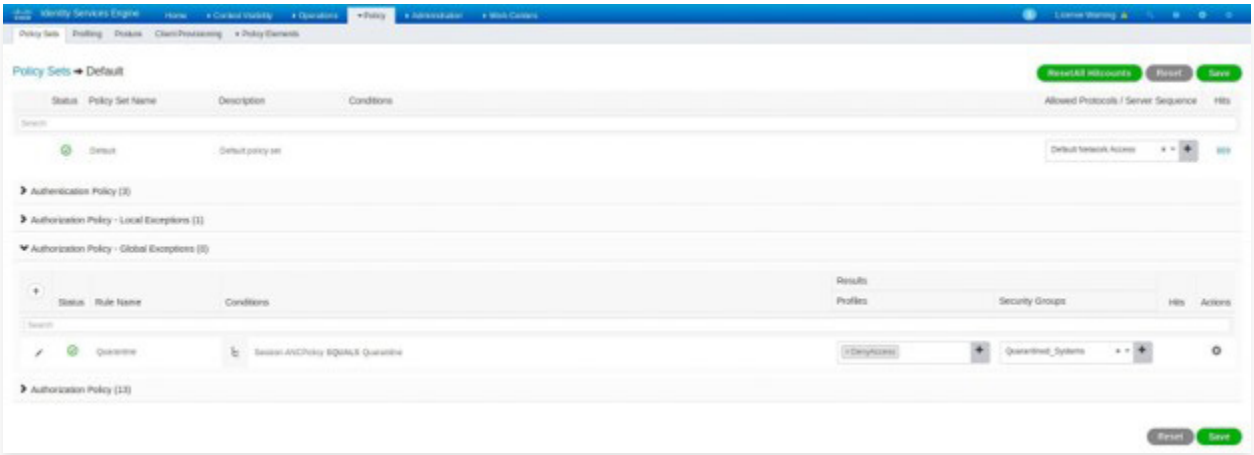


Figure 22: ANC Quarantine Authorization Policy - 2

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.

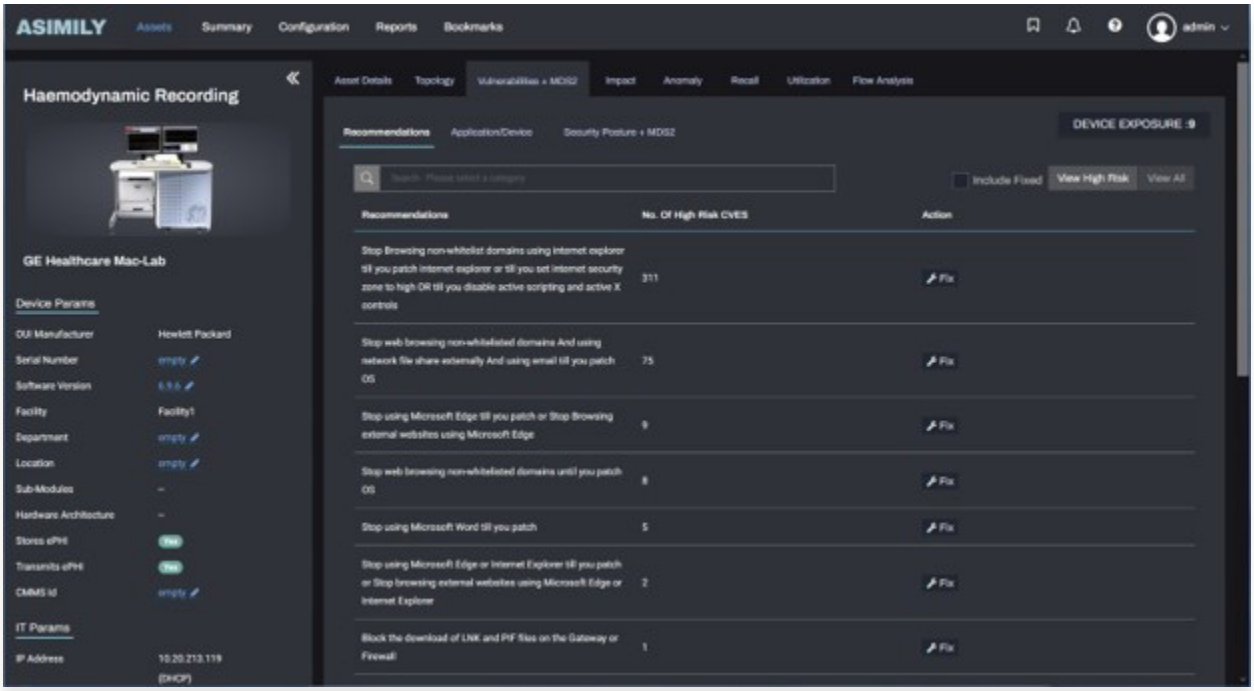


Figure 23: Recommendations for High Risk Vulnerabilities

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.

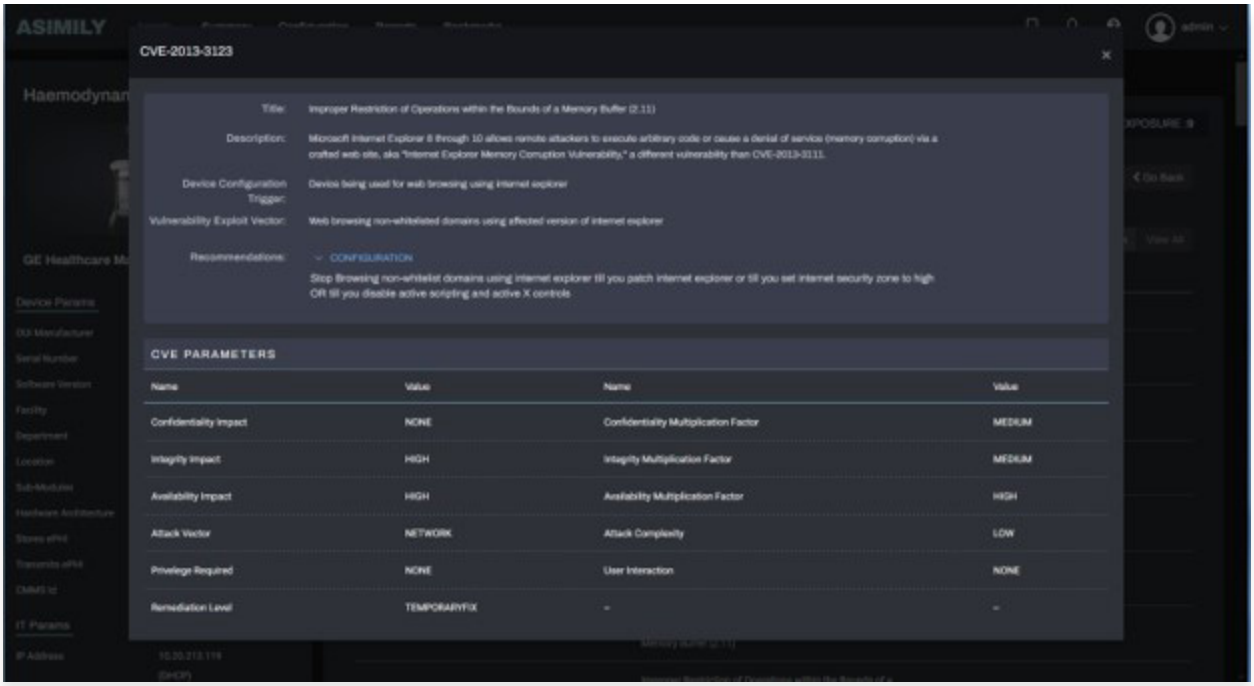


Figure 24: Exploit Vector, Device Configuration Trigger, and Recommendations for a CVE

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.

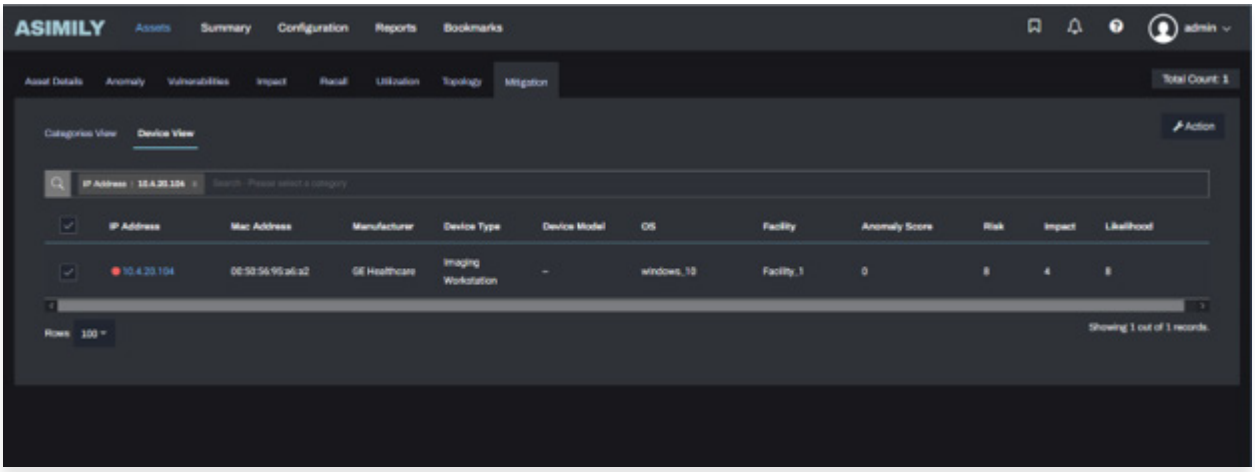


Figure 25: Exploit Vector, Device Configuration Trigger, and Recommendations for a CVE

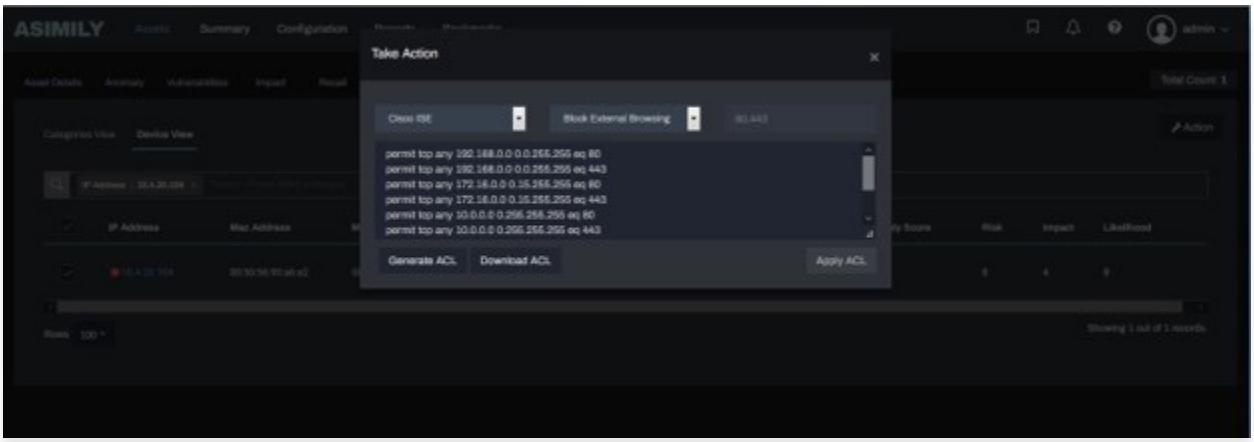


Figure 26: Exploit Vector, Device Configuration Trigger, and Recommendations for a CVE

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.

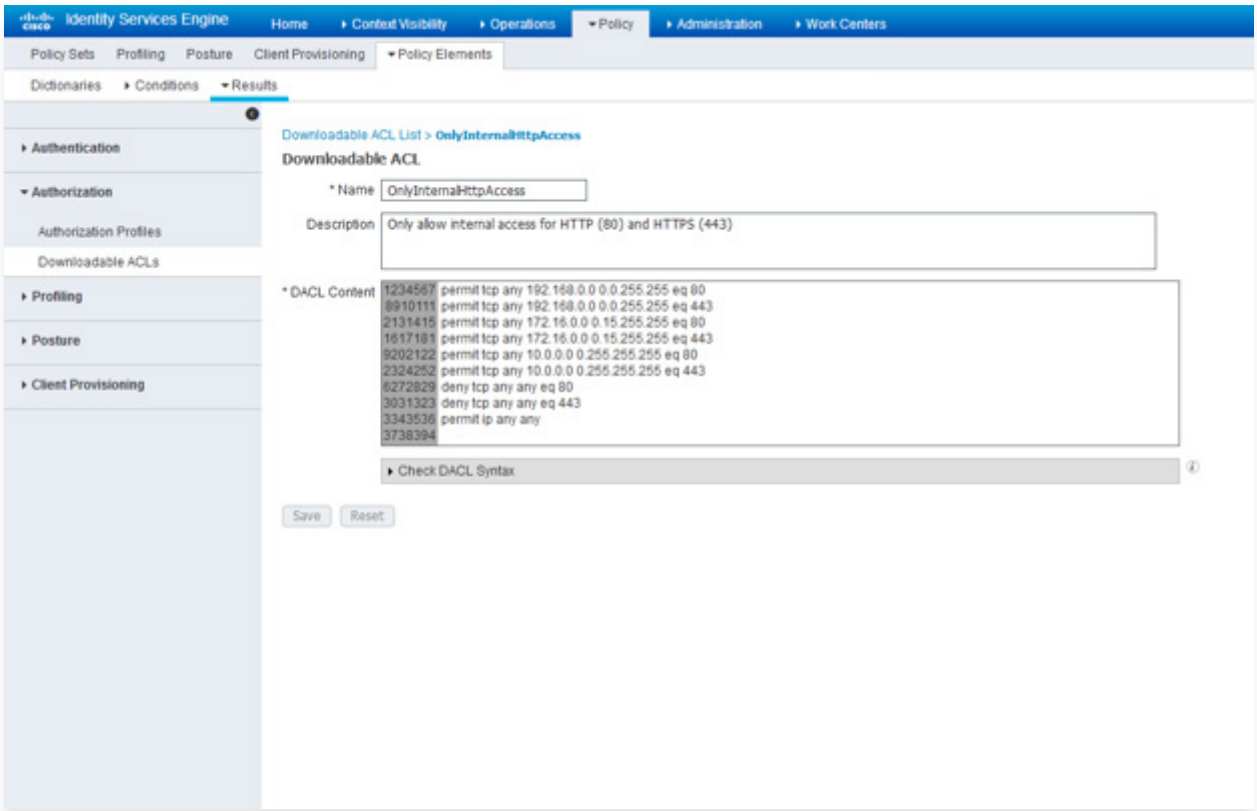


Figure 27: Creation of Downloadable ACL

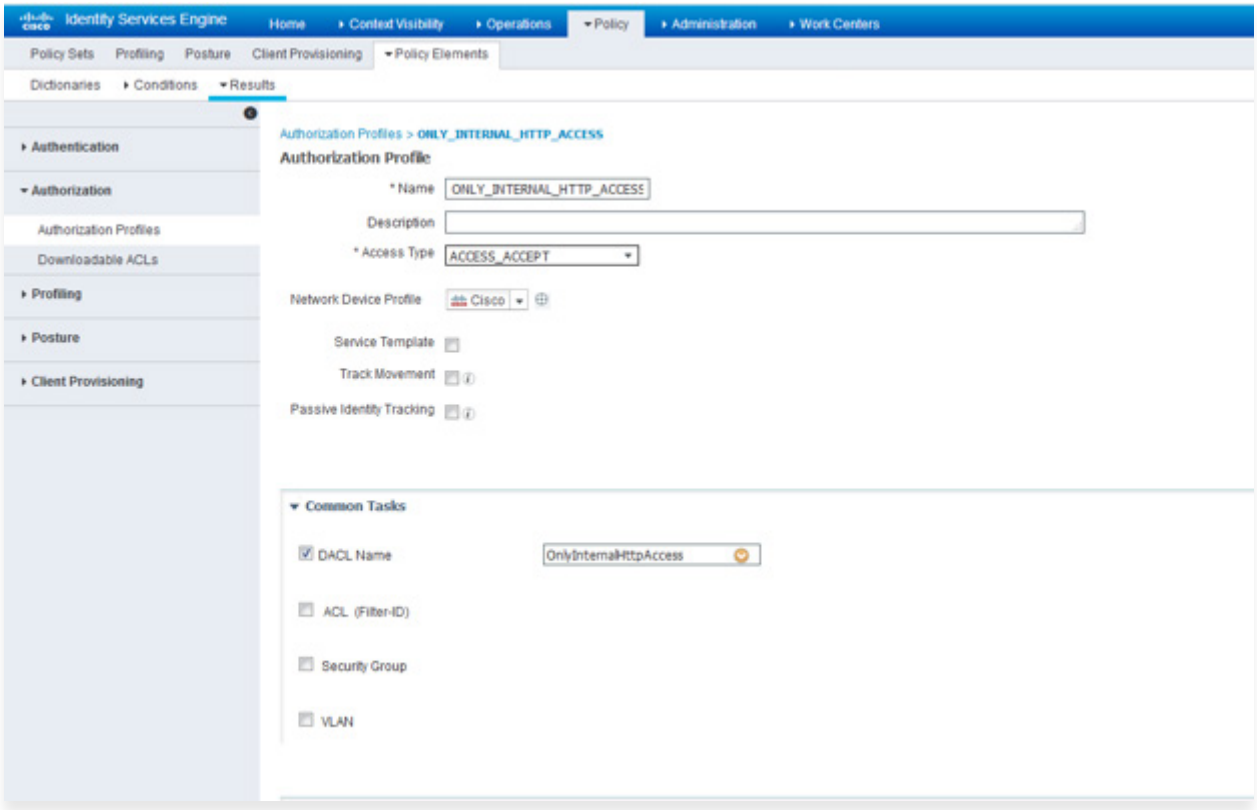


Figure 28: Create Authorization Profile and associate with DACL

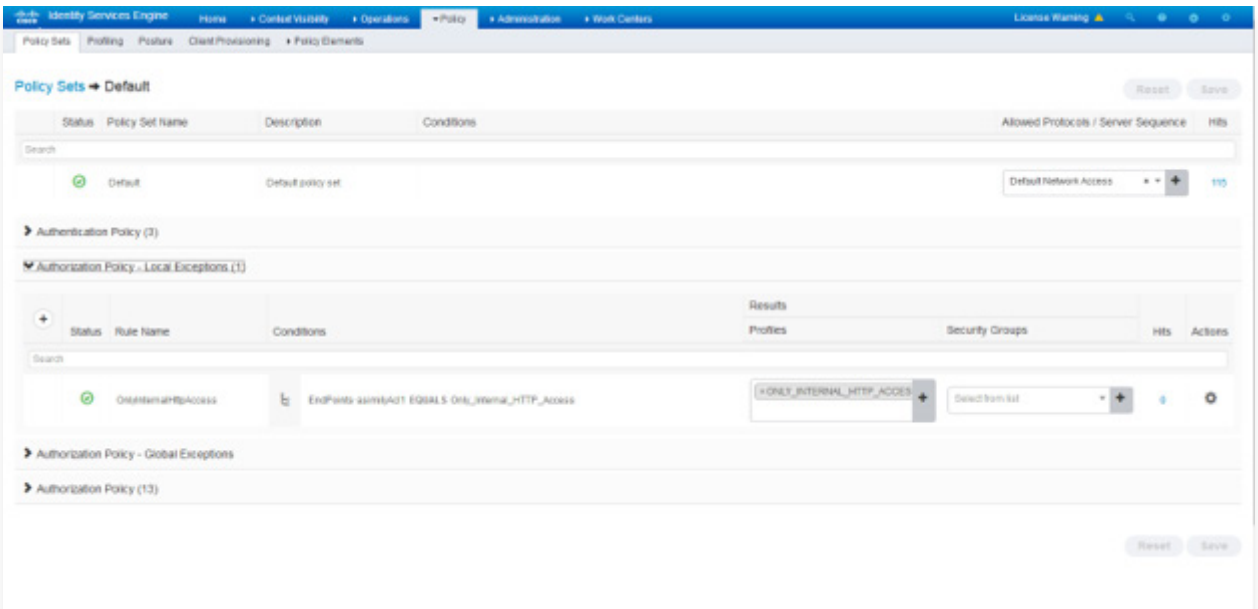


Figure 29: Create Authorization Policy and associate with Authorization Profile

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.

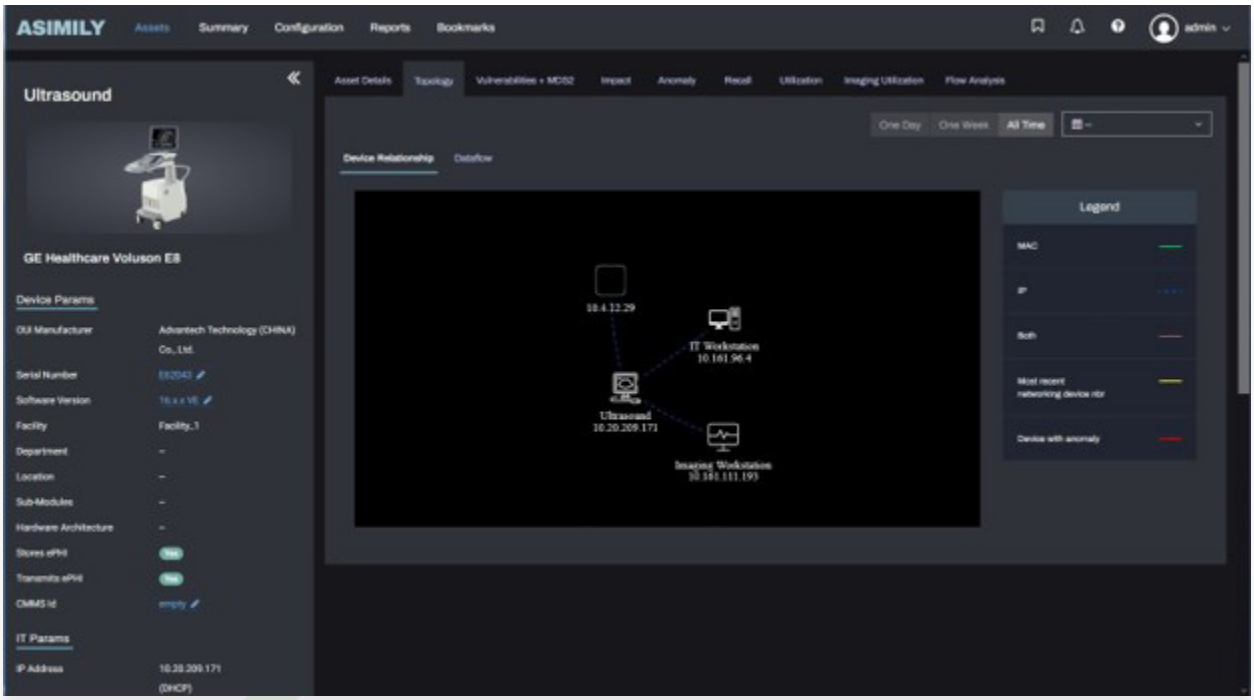


Figure 30: Device Topology

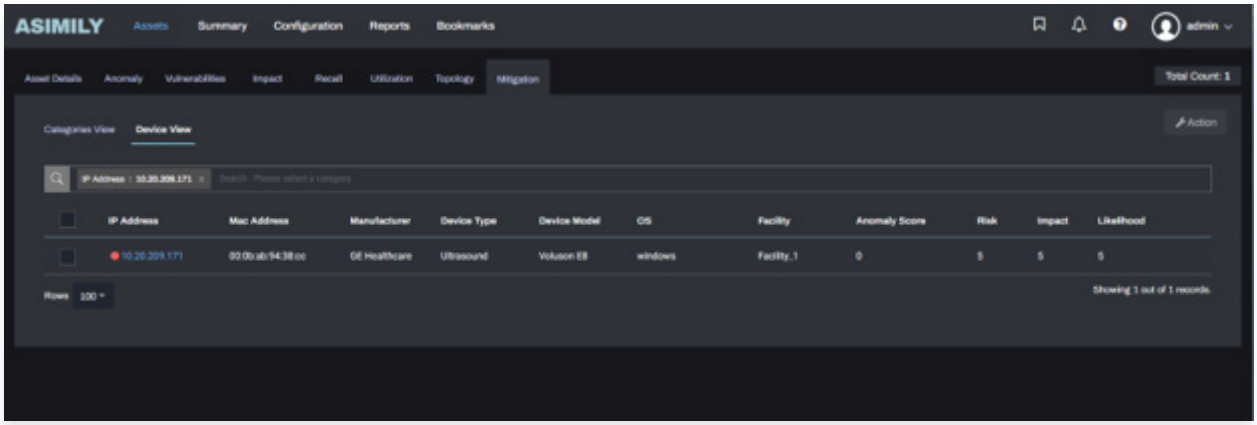


Figure 31: Mitigation – Device View

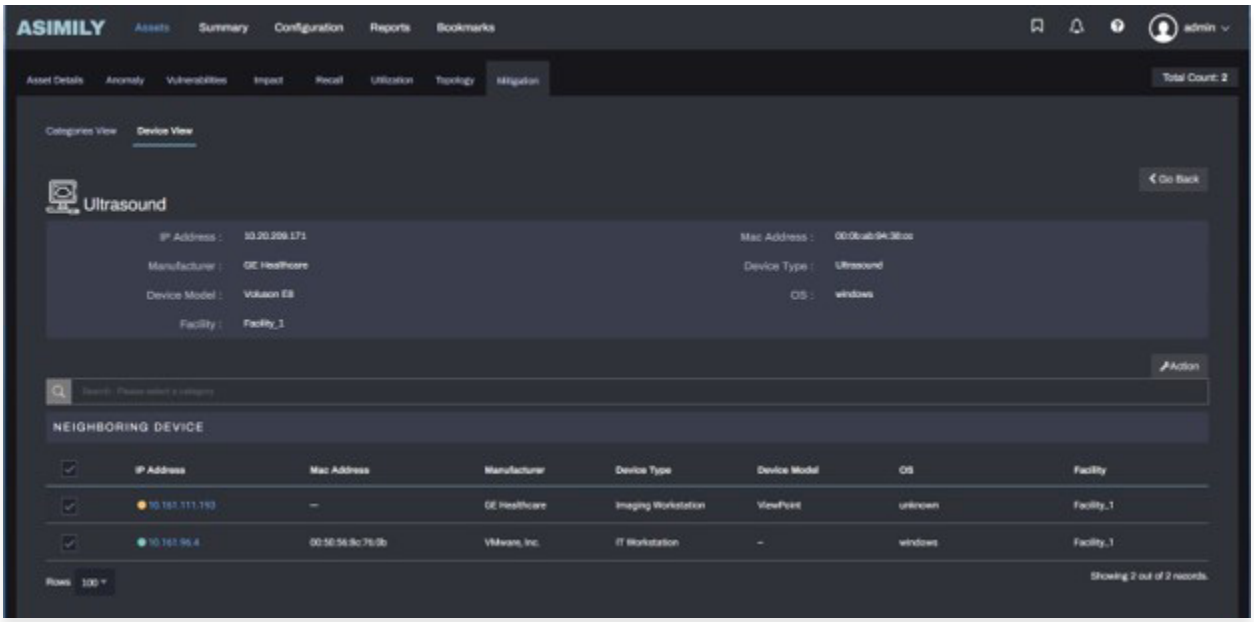


Figure 32: Mitigation – Device Topology View

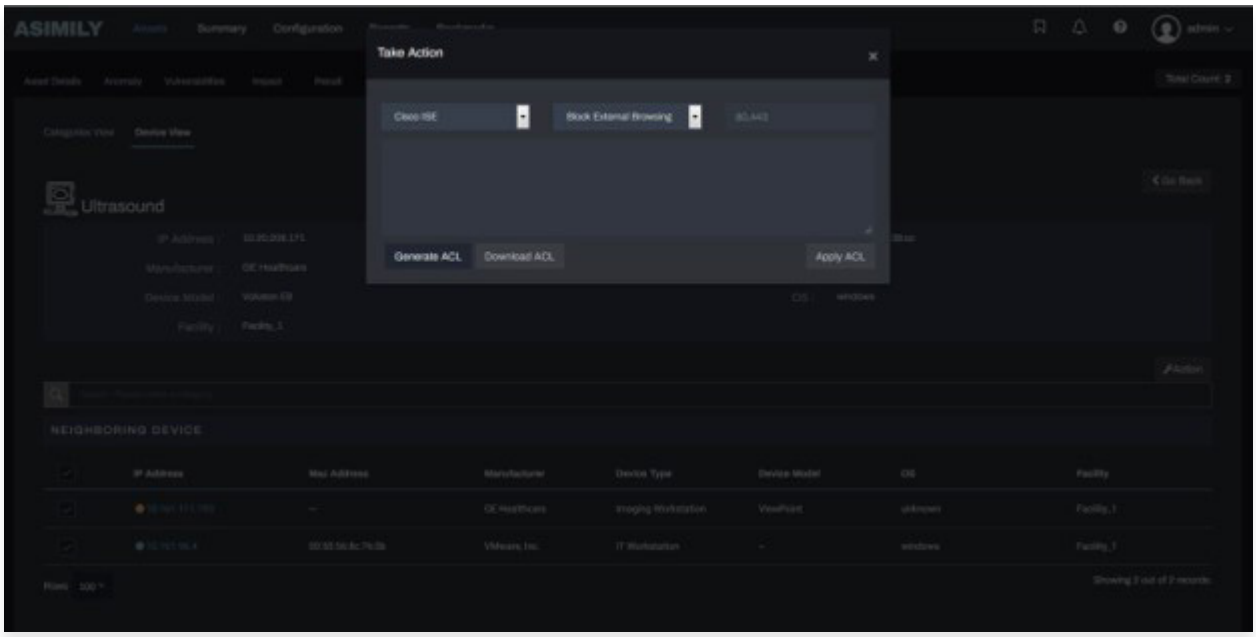


Figure 33: Device Topology View – Take Action

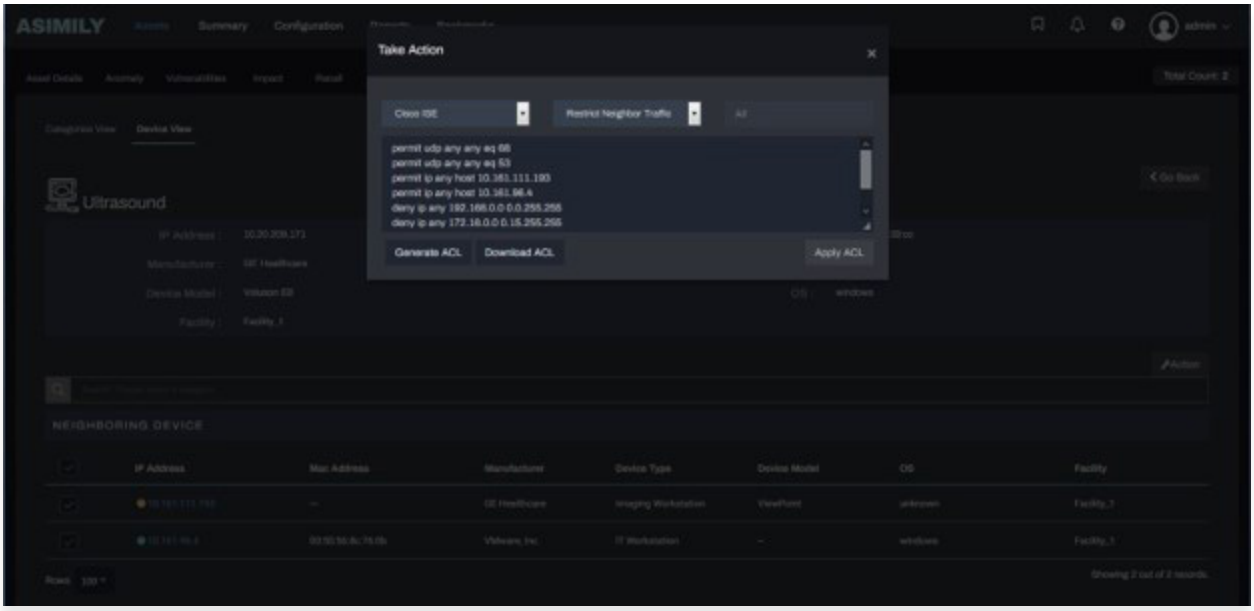


Figure 34: Device Topology View – Restrict Neighbor Traffic ACL

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.

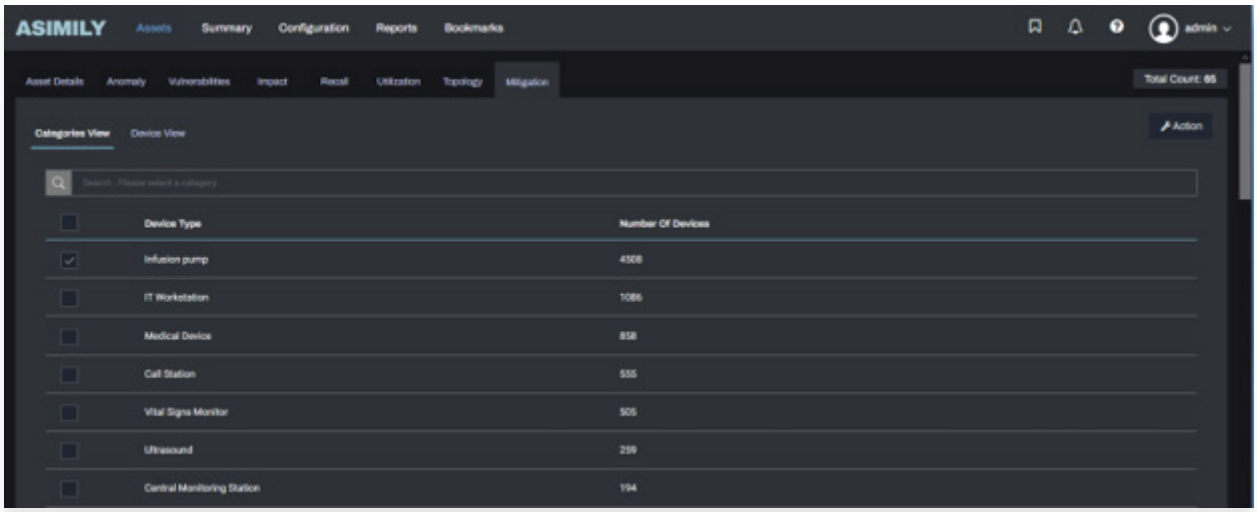


Figure 35: Mitigation – Category View

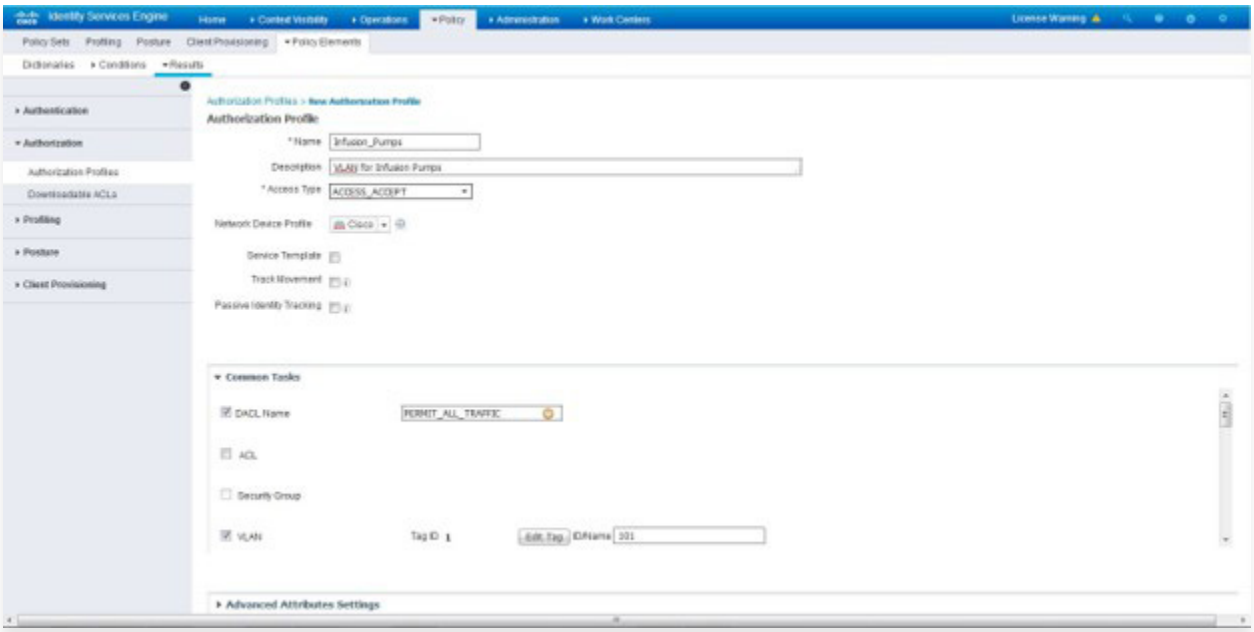


Figure 36: Create Authorization Profile – Assign VLAN ID

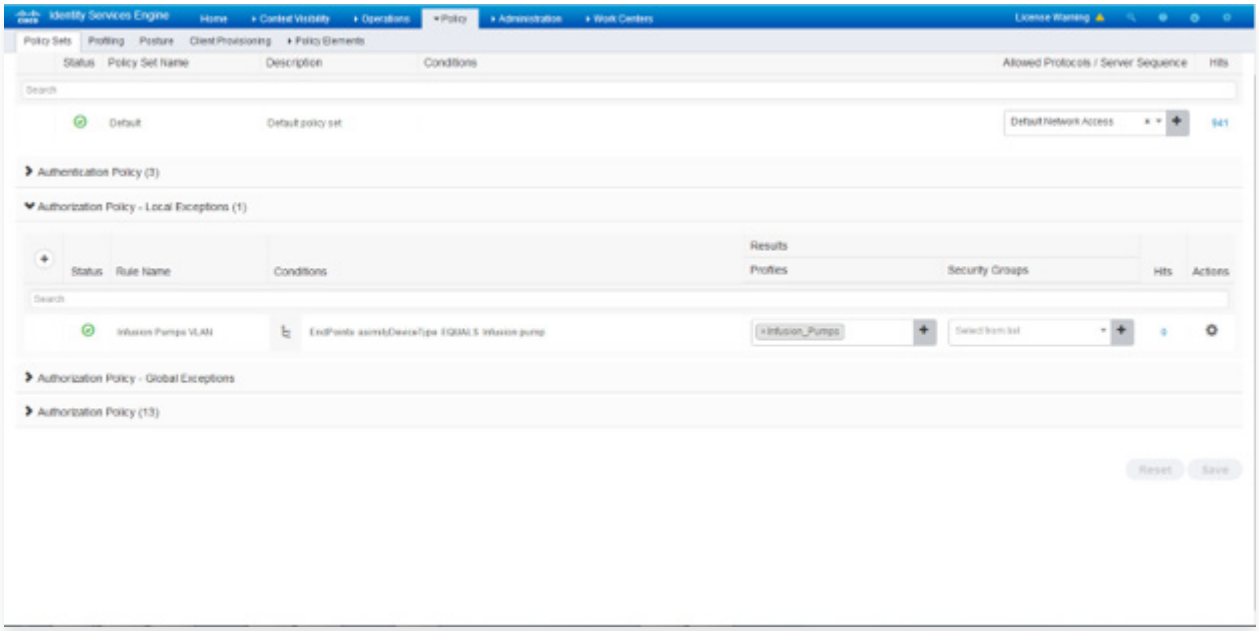


Figure 37: Create Authorization Policy – Infusion Pumps on specific VLAN ID

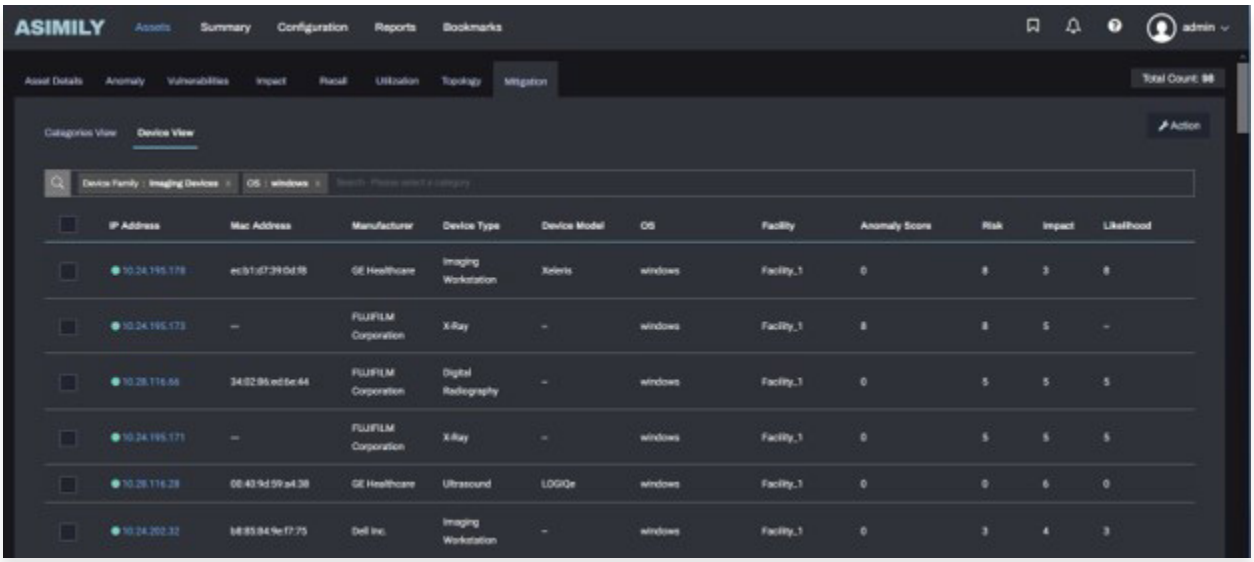


Figure 38: Select Imaging Devices with Windows OS

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 445

  deny tcp any any eq 2049

  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 445

deny tcp any any eq 2049

deny tcp any any eq 20

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 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, **arrange a demo today and a free Pre-procurement Risk Assessment for one model of your choice.**

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.