White Paper

Cisco Medical NAC

Identifying, Classifying, and Segmenting Clinical Healthcare Devices

Table of Contents

Introduction

What Is the Cisco Medical NAC?

Cisco® Medical Network Access Control (NAC) is a highly secure network access and policy management solution. It is designed to meet the specific needs of healthcare providers. Network access for both users and equipment typically spans many areas. Administrators, physicians, nurses, laboratory scientists and technicians, patients, visitors, partners, support staff, and other users need reliable and secure connectivity. An even larger list of nonuser devices must also securely connect to the network. These include critical-care devices, the network infrastructure, building automation and control, printers, phones, cameras, power control, point-of-sale, and entertainment systems.

Granting the appropriate level of access to both users and devices based on their functions and roles is critical if an organization wishes to provide secure and differentiated control to its resources on one common network.

Healthcare providers must also adhere to strict privacy laws and guidelines. These include the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS), which safeguard patient medical, financial, and electronic protected health information (ePHI). These laws and requirements, along with mandates from regulatory bodies such as the Food and Drug Administration (FDA), aim to ensure that each endpoint that connects to the network is detected, validated for compliance, and given access only to its intended resources. Healthcare organizations risk serious civil and criminal penalties for each breach incident. The total cost can spiral into the millions of dollars when the cost of notification, class action suites, remediation, and loss of business are taken into account. [Reference: Calculating the Cost of a HIPAA Data Breach]

In addition to protecting patient information, healthcare organizations must also protect clinical devices: the devices and systems responsible for the delivery of treatment. To meet these demands, it is often necessary to isolate both medical devices and user traffic by function and sensitivity to avoid exposure or interference between them. For example, a patient's personally identifiable information (PII) must not be accessible to nonauthorized parties. Billing and patient records should be kept separate and protected. And infusion pumps and patient monitors must be segregated from other networked hosts to prevent accidental or deliberate exposure and tampering.

To deliver secure network access to each of these users and devices, a comprehensive access and policy control solution must be implemented to address these key requirements:

- Identification and classification of all devices that connect to the network
- Strong authentication and authorization for all medical and supporting staff
- Compliance validation for staff members to validate current patches and client security software are installed and up to date
- Guest management system to allow simple but secure access to patients and visitors
- Device registration and onboarding of new corporate and personal assets
- Effective enforcement controls at the point of access and throughout the network
- Continuous monitoring and visibility for all network access, violations, and vulnerabilities
- Ability to detect threats and provide automated alerts and responses

Core components of the Cisco Medical NAC solution include the following:

- Cisco Identity Services Engine (ISE) for advanced visibility, policy management, and access control
- Cisco TrustSec® software-defined segmentation for visibility, and access control
- Cisco AnyConnect® clients for highly secure mobile connectivity on and off the healthcare network
- Cisco infrastructure and security devices to deliver reliable and highly secure access
- Technology partners that share rich contextual data with Cisco ISE to deliver superior visibility, threat detection, and containment

The Challenge of Securing Medical Devices

The healthcare industry faces unique challenges when it comes to the identification, classification, and authentication of medical devices. Rigid FDA guidelines prevent tampering with or modifying the hardware and software on these devices without a formal submission. With a primary focus on clinical function over security, manufacturers have failed to implement the most rudimentary forms of protection. Features that are often missing include operating system hardening, patch updates, and client security services like personal firewall, antimalware, host intrusion prevention, or authentication services like an 802.1X supplicant. It can be a time-consuming and costly process to validate compliance after a modification. Consequently, these devices are often deployed in an unprotected state, and manufacturers have little incentive to provide security updates as new vulnerabilities are discovered.

It is common to see medical devices that have been in operation for many years without any modifications that improve or address their security posture. These are the same devices responsible for the safety and health of the patients they serve. Their compromise or failure can result in a failure of the treatment or even death. However, awareness of the security gaps and risks in the healthcare environment has risen significantly. In the past couple of years individual testers have exposed the ease with which medical devices can be compromised or whose functions can be controlled without being detected, even devices that deliver critical care. For more details on the threat prevalence, refer to the article "It's Way Too Easy to Hack the Hospital," by Monte Reel and Jordan Robertson (November 2015).

With the stakes so high, healthcare delivery organizations are left with an enormous problem: how to ensure the safety of their patients—protecting both life and privacy—while having little control over the security of the devices used to treat and care for them.

The FDA mandates that "each manufacturer shall establish and maintain procedures for implementing corrective and preventive action." This directive may include the maintenance of the security baseline of medical devices such as security patches, antimalware, and encryption. The FDA further extends the responsibility of medical device manufacturers (MDMs) to off-the-shelf (OTS) software [Reference: Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software]. Unfortunately, not all MDMs are vigilant in updating their systems, and these mandates are at odds with the directive that prohibits device changes without formal submission. Once these devices are deployed, IT security administrators are typically unable or fearful to make updates and modifications to critical-care devices that could compromise the intended functionality or increase the risk of liability due to a malfunction.

Document Scope

Secure access to healthcare networks comprises many topics and technologies. This guide is focused on these specific topics:

- Secure-access options for healthcare-specific devices
- Identification and classification of healthcare-specific devices
- Extraction of data from existing sources
- Profiling methods and best practices
- Segmentation of medical devices

The terms “medical,” “healthcare,” and “clinical” are often used interchangeably when referring to network devices found in a healthcare organization. To clarify the scope of this document, the following terms will be used to distinguish medical device types:

- Healthcare IT: Supporting devices used in a patient care setting. Examples: nurse PC station or terminal, IP phone, label printer and bar code scanner
- Clinical devices: Devices directly related to the diagnosis and treatment of patients.

These devices can be further delineated as follows:

  - Non-life-critical: Devices used for diagnosis and treatment, but not directly involved in life-saving or life-sustaining functions. Examples: X-ray machine, CT scanner, ultrasound machine
  - Life-critical: Devices directly responsible for health monitoring and the delivery of life support functions. Examples: infusion pump, patient monitoring and telemetry, defibrillator

The focus of this guide is on best practices for the identification and classification of **clinical devices** and methods available to authenticate these devices to the healthcare network. This guide thus concentrates on the devices directly involved in the delivery of patient care and services. In addition to the above list of clinical devices, these endpoints include point-of-care, patient wearable, MRI, surgical, laboratory and diagnostic, nurse-call-system, and pharmaceutical devices.

Other healthcare IT devices such as network cameras, phones, environmental and building automation units, physical access control devices, and patient entertainment systems are critical to the overall healthcare operation but are outside the scope of this document. However, the principles discussed can be applied to the identification and classification of all devices that connect to the healthcare network.

This guide will also review methods to segment medical devices so that they protect data and services. Finally, this guide will introduce Cisco’s Medical NAC Profile Library along with step-by-step procedures to apply these healthcare profiles to your Cisco ISE deployment.

Secure Authentication for Medical Devices

When deciding how to identify critical-care devices on the network, you must first determine their capabilities. For example, does the device support 802.1X or another means like web portal or MAC authentication to identify itself to the network?

802.1X Authentication

In general, 802.1X is the preferred means of providing secure authentication to the network. If the device is 802.1X capable, the supported methods and protocols need to be determined. The key questions to be addressed include:

- Does the device support machine authentication, user authentication, or both?
- Which Extensible Authentication Protocol (EAP) types are supported? Common protocols include EAP TLS, EAP-TTLS, EAP-FAST, and PEAP, using the inner method EAP-MSCHAPv2, EAP TLS, or EAP-GTC. (These refer to, respectively, EAP Transport Layer Security, EAP-Tunneled TLS, EAP-Flexible Authentication via Secure Tunneling, Protected EAP, EAP-Microsoft's Challenge Handshake Authentication Protocol, EAP TLS, and the EAP-Generic Token Card.)
- What is the identity store (or certificate authority in the case of certificate-based identity) used for authentication and authorization?
- If multiple methods and protocols are supported…
  - Which options will best serve your organization's security requirements?
  - Which options will best serve your organization's operational model for deployment and maintenance?

Relatively few clinical devices support 802.1X for wired LAN connections. As more clinical devices take advantage of the mobility afforded by wireless LANs, it is expected that these devices will offer embedded EAP support. However, legacy systems often use less secure protocols like preshared key (PSK). While PSK is simple to configure, it is extremely vulnerable to password dictionary attacks. Furthermore, when a key has been compromised (through, for example, employee termination, accidental disclosure, or brute force attack), all devices that share that key are vulnerable and will need to be manually "rekeyed." We recommend that mobile medical devices still using PSK be updated to use more secure EAP methods if available.

Web Portal Authentication

Less common for medical devices is the use of some interactive portal that allow a user to enter credentials in a captive portal page. This method is less secure than 802.1X but more secure than simple MAC-based authentication. One advantage of web authentication is that it can force an interactive identification process rather than relying on a cached credential. However, this interactive requirement may be deemed a disadvantage as automatic, hands-off connectivity is typically a requirement for most clinical devices. Again, this method is not typically implemented for clinical or other healthcare devices, but is cited here for completeness on possible methods.

Note: Physicians, nursing staff, and other clinicians must often input their user or group-specific credentials to gain access to a terminal or medical application, but this is usually an application-based authentication, not a network-based authentication. Terminals and workstations that require user authentication to access clinical and patient care applications should also have a network-based authentication component, whether it is 802.1X, web, or MAC based.

MAC Authentication

Identification of an endpoint based solely on the MAC address is one of the most popular methods used to authenticate medical devices. The term “MAC authentication” is a bit of a misnomer. No true authentication occurs. Rather, a simple lookup from a local or centralized database of MAC addresses determines whether the address in question is authorized to access the network. Cisco refers to this method as MAC Authentication Bypass, or MAB, to highlight the fact that authentication is actually being bypassed.

The endpoint may have additional attributes associated with it, such as a group membership or classification that can be used to assign access. As an example, all known X-ray, CT, and MRI devices may be assigned to an identity group called Medical Imaging, while all known point-of-care devices may be assigned to an identity group called Patient Monitoring. Different policies can be associated with devices in each class.

The typical authentication flow for medical devices on a wired network is as follows:

1. Device connects to the network and the switch attempts 802.1X authentication.
2. 802.1X authentication fails due to lack of supplicant response to the switch’s 802.1X queries.
3. Switch falls back to alternative authentication using MAC authentication.
4. Switch sends the host MAC address to an authentication, authorization, and accounting (AAA) server using the Calling-Station-ID, Username, and/or Password attributes in a RADIUS packet.
5. AAA server validates the MAC address in a local or external database and assigns a policy based on group membership or other attributes.

The remainder of this guide focuses on the identification and classification of medical devices based on MAC addresses.

Classification of Healthcare-Specific Devices

In the absence of explicit identity credentials for network authentication, IT administrators must often resort to using the MAC address as the primary method to detect and classify medical endpoints. Some healthcare providers already have an external inventory of their medical devices. If these external databases support direct integration with Cisco ISE, then lookups to authorized endpoints can be simplified. Cisco ISE has the ability to perform MAC lookup to the following databases and identity stores:

- Cisco ISE internal endpoint database
- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Mobile device management (MDM)
- RADIUS

If the data on authorized medical devices resides in a format not directly accessible to Cisco ISE, the information may be imported to the internal endpoint database by the file, LDAP, or an API.

Unfortunately, most healthcare providers lack a complete or updated database of their medical devices, including individual MAC addresses. Fortunately, there is still a way to dynamically populate the endpoint database and assign classifications and policies, namely, profiling.

What Is Profiling?

Profiling in Cisco ISE is the automated process of device discovery and classification. It is based on the use of collectors, called probes, as well as on other sources of endpoint context. Probes use specific methods and protocols to collect attributes about each endpoint. The specific information a probe collects depends on the protocol and method implemented.

Cisco ISE supports various probes, each capable of capturing different endpoint data. Raw data for a given endpoint is parsed and stored in the ISE internal endpoint database. Relevant endpoint attributes are then analyzed against a library of fingerprinting rules known as Profiler policies. Different attributes and rules can have different weighting factors in the final endpoint classification depending on the reliability of the data.

ISE Probes to Classify Healthcare Devices

Different profiling probes contribute different information about each endpoint. In some cases, the same data is collected by different probes. The challenge is to deploy the probes that optimize the collection while adding unique value to the classification. In addition to enabling specific probes in Cisco ISE, the network must be configured to support collection, and the collection points must include relevant data.

The Cisco ISE Profiler includes the following probes and context sources for collecting endpoint attributes used to classify medical devices:

- RADIUS
- SNMP
- DHCP
- HTTP
- DNS
- Network scan (Nmap)
- NetFlow
- AnyConnect® Identity Extensions (ACIDEX)
- Device Sensor

The following section reviews the probes available in ISE. It explains how they work, what data they collect, and how they are used in medical profiling. Some best practices for implementation are offered. For a more detailed review of ISE profiling and probes, please refer to the ISE Profiling Design Guide.

RADIUS Probe

The RADIUS probe parses RADIUS AAA requests sent to the ISE policy service node and extracts attributes such as the MAC and IP addresses along with other connection information such as the network access device, port, VLAN, and authentication method.

The MAC address is a basic but important attribute. The first three bytes of this 6-byte address defines the Organizationally Unique Identifier (OUI) that uniquely identifies a vendor, manufacturer, or other organization worldwide. Since many medical devices are manufactured by companies with a specialized focus on healthcare, the OUI can be extremely useful in detecting medical devices and in some cases the specific device type or function.

By acquiring the IP-to-MAC-address bindings of endpoints, the RADIUS probe facilitates the functions of other probes that rely on IP addresses, such as DNS, Nmap, HTTP, and NetFlow. It is also used to support the Device Sensor, discussed later in this guide.

If RADIUS-based device authentication is used, then the RADIUS probe is a simple and efficient method to collect endpoint data. If network devices are not configured for RADIUS authentication, then it is still possible to use RADIUS accounting only or to use SNMP to detect new devices as they connect to the network.

The major attributes gathered from the RADIUS probe are:

- MAC address (OUI)
- IP address (used by other probes)

The RADIUS probe is **enabled** by default.

Note: It is not necessary to use profiling if a policy based on RADIUS attributes is needed. ISE can authorize endpoints directly based on the RADIUS attributes communicated during the connection phase.

SNMP Probe

There are two Simple Network Management Protocol (SNMP) probes: SNMPTRAP and SNMPQUERY.

SNMPTRAP

The SNMPTRAP probe is primarily used to trigger the SNMPQUERY probe. As new endpoints connect to the network, the switch can be configured to generate SNMP traps that are sent to the ISE appliance. ISE then queries the switchport for more information about the endpoint.

Since RADIUS accounting packets can also trigger the SNMPQUERY probe, the use of SNMPTRAP is typically limited to deployments where RADIUS authentication has not yet been deployed or to cases where no RADIUS authentication is planned or supported. The SNMPTRAP probe is useful in ISE deployments in a discovery-only phase or where the primary goal is simply to establish visibility into what is connected to the network.

Cisco ISE can process SNMP linkup and MAC notification traps as well as SNMP informs. MAC notification traps can populate the MAC address into the internal endpoint database without further interaction from SNMPQUERY or other probes. The inform and linkup trap provide ISE only with the switchport of the endpoint. Collecting MAC addresses and other endpoint data needs the SNMPQUERY probe to be enabled.

The SNMPTRAP Probe is **disabled** by default.

Best practice: Disable SNMPTRAP if RADIUS is already used to detect new endpoints.

Best practice: Configure access switches to send SNMP traps to only one or at most two ISE appliances to limit traffic and ISE replication. Using load balancers or Anycast can reduce the SNMP target list to one while still providing redundancy.

SNMPQUERY

The SNMPQUERY probe is used to perform three functions:

- **To trigger an SNMP query against a switchport** to acquire port details including interface number and VLAN, MAC-to-IP-address binding, and CDP/LLDP MIB information.

The main attributes gathered from the SNMPQUERY probe are:

- MAC address (OUI)
- IP address (used by other probes)
- CDP (cdpCacheCapabilities, cdpCacheDeviceId, cdpCachePlatform, cdpCacheVersion)
- LLDP (lldpCapabilitiesMapSupported, lldpChassisId, lldpSystemName, lldpSystemDescription)

In addition to current MAC and IP address-binding information, the information from both CDP and LLDP is extremely valuable profiling data. Common devices that generate CDP and LLDP data include infrastructure and voice and video endpoints.

From a pure medical device profiling perspective, the use of CDP and LLDP is limited. However, it is extremely valuable in identifying critical-support devices in healthcare, such as IP phones, cameras, call systems, and connected switches, and wireless controllers and access points.

- **To poll an SNMP query against a network access device** to detect all endpoints that do not or have yet to trigger a RADIUS event or SNMP trap. Upstream Layer 3 network devices can also be polled if they contain ARP tables for endpoints connected to Layer 2 switches.

The main attributes gathered from the SNMPQUERY probe are:

- MAC address (OUI)
- IP address (used by other probes)

SNMP polling is most valuable in discovering the MAC addresses of endpoints that rarely or never trigger a new connection event, to acquire the IP addresses of endpoints configured with a static IP address, and to acquire MAC-to-IP-address bindings for Layer 2–only switches.

Note: Each access device or Layer 3 device to be queried by ISE using SNMP must be added to the list of network access devices with a valid SNMP read community string.

- **To trigger an SNMP query against an endpoint** to acquire local system information as the result of an Nmap scan. If the Nmap probe detects that SNMP ports are open on the endpoint, it can trigger the SNMP query for more details like name, description, and location.

The main attributes gathered from the SNMPQUERY probe are:

- sysName
- sysDescr
- sysContact
- sysLocation
- hrDeviceDescr

A triggered SNMP query from an Nmap scan is most valuable for endpoints that support SNMP agents to track device details and operational status.

Note: To collect endpoint SNMP data as a result of the Nmap probe, ISE must be configured with the SNMP read community strings of endpoints to be queried.

Caution: Depending on the endpoints to be profiled, some healthcare organizations may prohibit the use of an active query against medical devices. Due to the critical nature of some clinical endpoints and the fact that many are not updated on a regular basis, there is some concern that the query may trigger a service disruption or even device failure.

Other devices that provide an ancillary or supporting role such as Windows or Linux workstations may be acceptable candidates for SNMP query.

The SNMPQUERY probe is **enabled** by default.

Best practice: When available, use the Device Sensor to collect CDP, LLDP, and other endpoint attributes. (The Device Sensor is discussed later in this guide.)

DHCP Probe

The Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses dynamically to hosts on a network. Although commonly used to provide an arbitrary address from a pool of addresses, it can also reserve IP addresses within a pool for use by specific endpoints. Consequently, DHCP provides central management of IP addresses for both random assignment across a shared pool as well as static assignment (DHCP reservation) for devices that require a deterministic IP address.

Cisco ISE includes two DHCP-based probes: DHCP and DHCPSPAN.

The DHCP probes are used to collect MAC addresses, IP addresses, and various option fields sent in standard DHCP packets. The primary difference between the two options is in the method used to send DHCP traffic to the ISE appliance. The DHCP probe is used when the Discover, Request, or Inform packet is relayed directly to the IP address of the ISE appliance. DHCPSPAN is used when a mirror of DHCP traffic is sent to a dedicated ISE appliance interface using a Switched Port Analyzer (SPAN) port or a network tap.

Most Layer 3 network devices can relay DHCP requests to a remote server. The DHCP probe is generally recommended for use with network devices capable of DHCP relay, especially when multiple distributed ISE appliances or DHCP servers are deployed. This removes the requirement for a single chokepoint, distributes the profiling load, and simplifies redundancy. For this configuration, the local default gateways for the access layer are configured with helpers or relays to send an extra copy of the DHCP packets to one ISE appliance (or two for redundancy). The ISE appliances do not respond to these packets. They only parse them for endpoint DHCP data.

The DHCPSPAN probe can be useful in the initial discovery phase and when all DHCP traffic travels through a specific “chokepoint” in the network, such as inline to a central DHCP server.

Best practice: When it is available, use the Device Sensor to collect CDP, LLDP, and other endpoint attributes. (The Device Sensor is discussed later in this guide.) When the Device Sensor is not available, use the DHCP relay and configure local Layer 3 gateways with helpers to send a copy of the DHCP request to one or at most two ISE targets. Load balancers or Anycast can be deployed to optimize distribution, increase redundancy, simplify network configuration, and trim the number of ISE targets to reduce data replication.

The main attributes gathered from DHCP and DHCPSPAN probes are:

- MAC address (OUI)
- IP address (used by other probes)
- Endpoint host or device name (hostname)
- Fully qualified domain name (FQDN) (client-fqdn)
- dhcp-class-identifier
- dhcp-user-class-identifier
- dhcp-parameter-request-list

The DHCP probe is **enabled** by default. The DHCPSPAN Probe is **disabled** by default.

DHCP attributes are valuable in detecting endpoint operating system types through the combination of attribute values or, in the case of the DHCP option parameter request lists, the specific order of numerical values. Unique combinations provide a fingerprint that enables profiling to classify devices by operating system or device type.

In some cases, manufacturers or network administrators populate specific fields in the DHCP requests that help identify the specific vendor, device model, or organization. For example, Sonosite, a major supplier of ultrasound machines, includes the name of its MicroMaxx product into the DHCP Class ID field. Similarly, Masimo, a leading manufacturer of patient monitoring devices, embeds the name MasimoSET in its line of SET pulse oximeters used to measure the amount of oxygen carried in the body.

Note: Refer to the DNS probe for more details on the benefits of the hostname and FQDN attributes.

Many medical devices are configured with static IP addresses. However, the growing popularity of mobile clinical devices has increased the number of medical devices that rely on DHCP to obtain an IP address. A side benefit of this trend is the availability of DHCP data for device classification.

Best practice: In situations where a specific IP address must be used for a device, DHCP reservations are recommended. DHCP reservations provide the benefits of centralized IP address management while allowing “static” or reserved IP addresses to be allocated to specific devices. Administrators responsible for manually updating static IP address assignments across many clinical devices will appreciate the benefits of DHCP reservations. In addition to significant time and cost savings, reservations can enhance profiling results.

HTTP Probe

The HTTP probe extracts the user agent string from a web-enabled application such as a browser or other application communicating over HTTP. The user agent commonly provides detailed platform and operating system details about the endpoint.

HTTP traffic can be captured and parsed by ISE appliances through URL redirection of endpoint web requests, such as occurs in central web authentication or hotspot guest access, or through direct requests to ISE portals, including the guest, sponsor, or My Devices portal. HTTP traffic can also be mirrored from a switch to dedicated ISE appliance interfaces using SPAN or network taps.

Note: The IP address of the endpoint must be known in order to associate HTTP traffic to the endpoint's MAC address. The exception is URL-redirected traffic where the ISE appliance directly correlates client HTTP/S requests to an existing endpoint session.

The main attribute gathered from an HTTP probe is:

- User-Agent (browser string)

The HTTP probe is **disabled** by default.

Note: Even if it is disabled, the HTTP probe still automatically parses web traffic that is sent to the IP address of an ISE appliance interface where profiling services are enabled. The HTTP probe should be enabled to parse HTTPS traffic sent to other targets such as mirrored SPAN traffic or local HTTPS traffic promiscuously captured by an ISE appliance interface.

Best practice: When it is available, use the Device Sensor to collect HTTP and other endpoint attributes from the network access devices. (The Device Sensor is discussed later in this guide.)

DNS Probe

The DNS probe is triggered when the IP address of an endpoint is learned. The probe queries the name server configured on the ISE appliance to resolve the hostname or FQDN assigned to the IP address. This request is commonly known as a reverse host or reverse DNS lookup.

Many organizations have well-defined naming conventions that they use to assign specific names or strings to their network hosts to quickly identify location, responsible group, or device type. For example, the hostname maybe assigned a prefix of "MRI" or "CT" to indicate that it is an imaging device. The subdomain may be assigned to a specific clinical organization, as in "biomed.ogranization.org."

In some cases the manufacturer of the medical device may populate the hostname with a default value to indicate the vendor or device model.

The main attribute gathered from the DNS probe is:

FQDN (hostname + domain name)

The DNS probe is **disabled** by default.

Best practice: It is recommended that the DNS probe be deployed if medical devices have or can be made to have a well-defined name format and if these names populate the organizational name servers either statically or dynamically (through dynamic DNS).

The endpoint hostname and FQDN may also be acquired by the DHCP probe. Of the two sources of information, DNS probe data is more reliable and trustworthy. DHCP options are submitted by the client, whereas the DNS probe acquires information from the DNS name server.

Nmap Probe

The Network Scan probe is based on the open source “network mapper,” or Nmap. Over many years of community contribution, Nmap has expanded and matured into a powerful scanning and endpoint enumeration tool.

The Nmap probe is commonly used to detect open ports that indicate the presence of specific applications and services and to detect operating systems. ISE also uses this probe to determine whether the host is running an SNMP agent. If so, additional SNMP queries can be sent to collect more details about the endpoint. (For more information on SNMP query data collection, refer to the SNMPQUERY section under SNMP Probe.)

The main attributes gathered from the Network Scan (Nmap) probe are:

- Common ports (including 16 UDP ports and 18 TCP ports, fixed)
- Operating system
- SNMP endpoint query attributes (see the section on SNMPQUERY probes)

The Nmap Probe is **enabled** by default.

Caution: Depending on the endpoints to be profiled, some healthcare organizations may prohibit the use of an active scanning tool against medical devices. Due to the critical nature of some clinical endpoints and the fact that many are not updated on a regular basis, there is some concern that the scan may trigger a service disruption or even device failure.

Other devices that provide an ancillary or supporting role such as Windows or Linux workstations may be acceptable candidates for an Nmap scan.

Best practice: Review the risks and potential benefits of permitting an active Nmap scan against healthcare endpoints.

NetFlow Probe

NetFlow is protocol designed by Cisco. NetFlowIt is widely implemented across the industry in routers, switches, and other network devices to monitor the type of traffic sent to and from various hosts on the network. It is an extremely powerful tool for the collection and analysis of network traffic.

The NetFlow probe allows ISE to collect and make policy rules based on this flow data. The other probes discussed to this point rely mostly on information originated by the endpoint. In contrast, the NetFlow probe is able to learn the actual traffic patterns of the endpoint. This capability uniquely allows ISE to classify endpoints based on behavior, not on attributes of the endpoint itself.

The NetFlow probe has a number of critical benefits in the healthcare environment, including:

- **Profiling of endpoints that cannot be identified with traditional profiling methods**. For example, a monitoring station for infusion pumps may run on a general-purpose hardware platform and operating system kernel. In such cases, only a generic profile, if any, is possible. A lack of DHCP, DNS, and Nmap data further limits what can be gleaned from the endpoint. Tracking network communications to infusion pumps on specific ports offers a traffic fingerprint of the device.
- **Increased profiling fidelity to complement data acquired through traditional methods**. For example, an infusion pump may be detected by a unique MAC address (OUI), but its communication to a monitoring

station on specific ports expected for that device increases the confidence of the data regarding device type and function.

- **Classification based on expected behavior or unexpected behavior (anomalous traffic).** For example, when the infusion pumps and monitoring station described in the above examples operate within a predicted pattern, there is assurance that the devices are operating normally. If these same devices communicate outside their expected boundaries over foreign ports and different targets, that is an indication that these critical devices may have been compromised, thus triggering an alarm and optional reclassification or even quarantine.

Traditional profiling methods include the use of SNMP, DHCP, HTTP, and other common protocols. These methods often lead to a knowledge of the OS type or hardware manufacturer. In the case of medical devices built on general-purpose hardware and operating system software, this information may provide little value in differentiating a Windows workstation used for a medical application from one used for nonclinical applications.

ISE ships with a number of medical profiles based on NetFlow data. These include patient monitoring devices developed by Philips and Draeger as well CareFusion pumps. Additional medical profiles can be added or enhanced in ISE by inputting the specific UDP or TCP ports used by these devices.

The main attributes gathered from NetFlow probes are:

- IPV4_SRC_ADDR (source IP address)
- L4_SRC_PORT (source port)
- IPV4_DST_ADDR (destination IP address)
- L4_DST_PORT (destination port)
- Protocol (UDP or TCP)

The NetFlow probe is **disabled** by default.

Best practice: Implement NetFlow profiling for specific medical devices with known traffic characteristics. Configure NetFlow sources where the medical device traffic must traverse the network. When possible, limit flow collection to the data of interest.

ACIDEX

The Cisco AnyConnect Identity Extension (ACIDEX) is not an explicit probe configured in ISE, but is yet another source of profiling data against which endpoints can be classified. The source of this data is currently limited to remote devices that establish a VPN connection to a Cisco Adaptive Security Appliance (ASA) using a Cisco AnyConnect client. This functionality is useful in profiling remote workstations and mobile devices.

The main attributes gathered from ACIDEX are:

- device-platform (example: iPad3)
- device-platform-version (example: apple-ios)
- device-type (example: 9.1)

ACIDEX attributes are forwarded from the ASA to ISE using RADIUS. Since the RADIUS probe is enabled by default, ACIDEX processing is also enabled on ISE by default.

Device Sensor

The Device Sensor is not a probe, but an optimization in the collection and reporting of endpoint attributes. Device Sensor is a feature that runs on the network access device such as Cisco Catalyst® switches and Cisco Wireless LAN Controllers.

The sensor locally captures attributes such as MAC address, IP address, CDP and LLDP details, DHCP option fields, and HTTP user agents. It then packages and reports these attributes in a RADIUS accounting updates packet. On switches, the Device Sensor can be configured to filter specific attributes of interest. Since all information is sent over RADIUS, ISE only requires the RADIUS probe to be enabled in order to process Device Sensor updates.

Note: The specific attributes supported by the Device Sensor will depend on the hardware platform and version. Refer to the documentation for your specific switches and wireless controllers.

The Device Sensor reduces the operational requirements for data collection on the network infrastructure. It reduces the amount of traffic and bandwidth that must be processed. And it improves ISE database scalability by reducing the number of updates to a specific ISE appliance.

Best practice: We generally recommend that you deploy the Device Sensor if it is supported by your network access device. Test the functionality first to verify that all attributes are reported as expected. If you receive the desired attributes, disable any duplicate methods of profile data collection for the endpoints connected to these network devices. For example, the Device Sensor is configured to send DHCP data. It is unnecessary to also forward DHCP packets using relays or helpers on the local switch or upstream gateway.

Summary of Probes

Table 1 summarizes the probes and other sources of endpoint attributes in Cisco Identity Services Engine profiling.

Table 1. Endpoint Attributes Collected by Cisco ISE Probes to Classify Healthcare Devices

Probe	Default ISE Setting	Main Attributes Collected
RADIUS	Enabled	• MAC address • IP address
SNMPTRAP	Disabled	• MAC address (MAC notification only)

SNMPQUERY	Enabled	• MAC address
		• IP address
		• CDP:
		  ◦ Capabilities
		  ◦ Device ID
		  ◦ Platform
		  ◦ Version
		• LLDP:
		  ◦ Capabilities map supported
		  ◦ Chassis ID
		  ◦ System name
		  ◦ System description

DHCP	Enabled	• MAC address • IP address • Endpoint host or device name

Probe	Default ISE Setting	Main Attributes Collected
		• FQDN • Class ID • User class ID • Parameter request list
HTTP	Disabled	• User agent
DNS	Disabled	• FQDN
Nmap	Enabled	• Common ports • Operating system
Nmap >> SNMP query	(Depends on scan action)	• System name • System description • System contact • System location • HR device description
NetFlow	Disabled	• Source IP address • Source port • Destination IP address • Destination port • Protocol
ACIDEX	Enabled (through RADIUS)	• Device platform • Device platform version • Device type
Device Sensor	Enabled (through RADIUS)	• MAC address • IP address • CDP • LLDP • mDNS • SIP • H.323

When deciding how best to classify devices using profiling, it is important to understand the basic characteristics of the device being profiled and the types of data it is capable of exposing to the network. This information will help determine which probes and collection methods are most appropriate for classifying the device. Common questions include:

- Is the device statically or dynamically assigned an IP address? If statically, is it possible to use DHCP reservations to assign a specific address while also collecting profiling data?
- Is it acceptable to actively scan the endpoint using Nmap, or could such a scan adversely affect the host?
- Does the device have a deterministic hostname format? Does the device have a DNS entry with a specific naming convention?
- Does the device have predictable traffic patterns? (For example, does a nurse's workstation always communicate to a known set of patient-monitoring devices?)
- Is the device directly connected to the IP network, or is it connected through another serial or wireless gateway device? In the both cases, it is necessary to profile the controller device rather than the actual medical device.

To assist with the tracking of such information, the Appendix includes a Medical Device Custom Profile Checklist that can be completed for each device. The checklist serves as a guide as to which profiling methods will be most effective for each device. It also provides the information you need to create custom profiling conditions and policies.

Cisco Medical NAC Profile Library

Overview

Cisco has developed about 500 canned profiles that use the various probes. The profiling library comes preconfigured in ISE and is continually updated using the automated Feed Service. ISE provides the ability to modify any of the canned profiles. Administrators can also create new customized profiles.

In addition to the default profiles, Cisco has created a special library of medical device profiles targeted for healthcare delivery organizations that can be downloaded from Cisco.com. The Cisco Medical NAC Profile Library will continue to evolve. As of February 2016 it contained more than 250 medical device profiles.

Cisco ISE Medical NAC Profile Library		
3M-Company-Device	Edwards-Lifesciences-Device	Olympus-Image-Systems-Device
3M-Deutschland-Device	Ellex-Medical-Device	Olympus-Soft-Imaging-Device
3M-Germany-Device	Essilor-Device	Omron-Healthcare-Device
Abbott-Diagnostics-Device	Fisher-Paykel-Device	Onyx-Healthcare-Device
Abbott-Medical-Optics-Device	Fluke-Biomedical-Device	Optimedical-Systems-Device
Abbott-Point-of-Care-Device	Fresenius-Medical-Care-Device	ORTHOsoft-Zimmer-CAS-Device
ACIST-Medical-Systems-Device	Fukuda-Denshi-Device	Ortivus-AB-Medical-Device
Acteon-Group-Device	Gambro-Lundia-Device	Oticon-Device
Advanced-Medical-Information-Device	GE-Healthcare-Device	Pacific-Biosciences-Device
Advance-Sterilization-Products-Device	GE-Medical-System-Device	PaloDEx-Device
Advantage-Pharmacy-Device	Gem-Med-Device	Palomar-Medical-Device
Aeroscout-Device	Getinge-IT-Solutions-Device	Panasonic-Healthcare-Device
Alaris-Inc-Device	Getinge-Sterilization-Device	Pharma-Smart-Device
Alaris-Medical-Systems-Device	GN-ReSound-Device	Philips-Analytical-X-Ray-Device
Alcon-Laboratories-Device	Haag-Streit-Device	Philips-CareServant-Device
Alpinion-Medical-Systems-Device	Health-Hero-Device	Philips-Healthcare-PCCI-Device
AmbiCom-Device	Health-Life-Device	Philips-Intellivue
American-Telecare-Device	Heart-Force-Medical-Device	Philips-Medical-Systems-Device
Andon-Health-Device	HemoCue-Device	Philips-Oral-Healthcare-Device
Applied-Biosystems-Device	Heraeus-Noblelight-Device	Philips-Patient-Monitoring-Device
Applied-Medical-Technologies-Device	Hitachi-Aloka-Medical-Device	Philips-Personal-Health-Device
ARKRAY-Device	Hoana-Medical-Device	Philips-Respironics-Device
Avizia-Device	Honeywell-HomMed-Device	Phonak-Communications-Device
Axis-Shield-PoC-Device	HORIBA-Medical-Device	Physio-Control-Device
Bang-Olufsen-Medicom-Device	Hospira-Device	Physiometrix-Device
Baxter-Healthcare-Device	Huntleigh-Healthcare-Device	Planmeca-Oy-Device
Bayer-HealthCare-Device	Imatron-Device	Pointe-Conception-Medical-Device
B-Braun-Melsungen-Device	Imricor-Medical-Systems-Device	Power-Medical-Interventions-Device
Beacon-Medical-Device	Indiana-Life-Sciences-Device	Progeny-Midmark-Device
Beckman-Coulter-Device	InnerSpace-Device	Proteus-Digital-Health-Device
Becton-Dickinson-Device	Innomed-Medical-Device	Quantum-Medical-Imaging-Device
Bestcare-Cloucal-Device	INSIDE-Technology-Device	Radiometer-Medical-Device
Biodevices-Device	INTEGRA-Biosciences-Device	ResMed-Device
Bio-logic-Systems-Device	Integra-LifeSciences-Device	Resurgent-Health-Medical-Device

bioMerieux-Italia-Device	Integrated-Medical-Systems-Device	RF-Surgical-System-Device
Bionet-Device	Intel-GE-Care-Innovations-Device	Robert-Bosch-Healthcare-Device
BIOPAC-Systems-Device	Interacoustics-Device	Robert-Bosch-Healthcare-GmbH-Device
Bio-Rad-Lab-Devices	Intuitive-Surgical-Device	Robert-Bosch-Healthcare-Systems-Device
Biosoundlab-Device	Invivo-Device	Roche-Diagnostics-Device
Biospace-Device	Ivoclar-Vivadent-Device	ScottCare-Device
Biotage-Device	Ivy-Biomedical-Device	Secure-Care-Device
Biotronik-Device	Johnson-Johnson-Medical-Device	SenTec-Device
BL-Healthcare-Device	Jostra-Device	Senticare-Device
BMT-Medical-Technology-Device	Karl-Storz-Imaging-Device	Shenzhen-Lifesense-Medical-Device
Boston-Scientific-Device	KaVo-Dental-Device	Shimadzu-Device
C8-MediSensors-Device	KeyMed-Device	SHL-Telemedicine-Device
Calypso-Medical-Device	Kollmorgen-Corp-Device	Siemens-AG-Healthcare-Sector-Device
Camtronics-Medical-Sytems-Device	Kollmorgen-Servotronix-Device	Siemens-Healthcare-Diagnostics-Device
CardioMEMS-Device	Kontron-Medical-Device	Siemens-Healthcare-Diagnostics-Manufacturing-Device
CardioNet-Device	LABiTec-Device	Sigma-International-Medical-Device
Cardiopulmonary-Corp-Device	Laerdal-Medical-Device	Sirona-Dental-Systems-Device
CardioTek-Device	Leica-Biosystems-Device	Smiths-Medical-Device
CareCom-Device	Leica-Microsystems-Device	SonoSite-Device
Care-Everywhere-Device	LI-COR-Biosciences-Device	Sonosite-MicroMaxx-Ultrasound
CareFusion-Alaris-Pump	LifeSync-Device	Soredex-Device
CareFusion-Device	LRE-Medical-Device	Spacelabs-Healthcare-Device
CarePredict-Device	Maquet-Cardiopulmonary-Device	Spectrum-Medical-Limited-Device
Carestream-Health-Device	Maquet-CardioVascular-Device	Sphere-Medical-Device
CareTech-Device	Maquet-Critical-Care-Device	Starkey-Labs-Device
CareView-Communications-Device	Maquet-GmbH-Device	St-Jude-Medical-Device
Celectronic-eHealth-Device	Marconi-Medical-Systems-Device	Stratec-Biomedical-Device
Centrak-Device	Masimo-Device	Stryker-Device
CHG-Hospital-Beds-Device	Masimo-SET-Pulse-Oximeter	Tecan-Systems-Device
Chile-School-of-Medicine-Device	MedAvant-Healthcare-Device	Terumo-Device
CIRTEC-Medical-Systems-Device	MedAvant-Healthcare-Solutions-Device	Thermo-Fisher-Scientific-Device
CliniComp-Device	MEDAV-Device	Thoratec-Device
Cogent-Healthcare-Systems	Mediana-Device	Tiba-Medical-Device
Colorado-Med-Tech-Device	Medicis-Device	Tokyo-Boeki-Medisys-Device
Compumedics-Device	Medicore-Device	Toyo-Medic-Device
Conmed-Linvatec-Device	Medison-X-Ray-Device	tPlus-Medical-Device
Convergent-Bioscience-Device	Medrad-Device	Trendsetter-Medical-Device
Corometrics-Medical-Systems-Device	Medtronic-Diabetes-Device	Tunstall-Healthcare-Device
Criticare-Systems-Device	Mennen-Medical-Device	Valtronic-Device
Cutera-Device	Micropoint-Biotechnologies-Device	Varian-Medical-Systems-Device
Dainippon-Pharma-Device	Mindray-Co-Device	Versamed-Device
Danaher-Motion-Kollmorgen-Device	Mindray-DS-USA-Device	Verto-Medical-Device
Datex-Ohmeda-Device	MIR-Device	VIASYS-Healthcare-Device
DENTSPLY-Gendex-Device	MOCACARE-Device	Vigil-Health-Solutions-Device
Diatek-Patient-Management-Device	Molecular-Devices-Corp-Device	VitalCARE-Device
Dictum-Health-Device	Mortara-Instrument-Device	Vocera-Device
Disetronic-Medical-Systems-Device	NDS-Surgical-Imaging-Device	Welch-Allyn-Device
Dixtal-Biomedica-Device	Neural-Image-Device	West-Com-Nurse-Call-Device
Draeger-Delta	Nicolet-Instruments-Device	Widex-Device
Draeger-M300	Nicolet-Neuro-Device	Zimmer-Elektromedizin-Device
Draeger-Medical-Device	Nihon-Kohden-Device	Zoe-Medical-Device
Draeger-Medical-Systems-Device	Nipro-Diagnostics-Device	ZOLL-Lifecor-Device
Dragerwerk-Device	Nonin-Medical-Device	
Durr-Dental-Device	Novo-Nordisk-Device	

Installing the Library

This section describes where to go to download the Cisco Medical NAC Profile Library and how to install it.

Downloading the Library

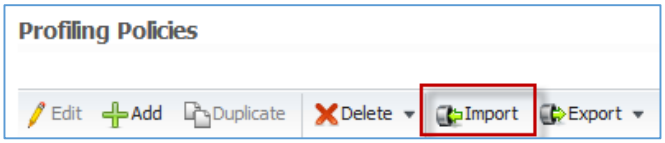
Cisco generally uses the Profiler Feed Service for publishing and automatically distributing new profiles to customer ISE deployments. The Feed Service is intended to provide a benefit to all customers through the refinement and addition of new profiles used to classify endpoints in any environment. Because the Medical NAC Profile Library is specific to devices in a healthcare network and contains many profiles that may not be of interest to the general customer, the medical library is posted to a community forum. Healthcare and other interested organizations can access and apply the profiles as needed.

The Cisco Medical NAC Profile Library is posted to the Cisco community forum at: https://communities.cisco.com/docs/DOC-66340.

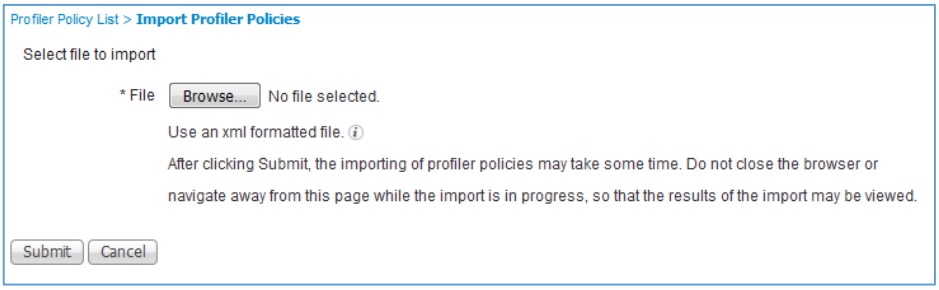
Download and save the file to a directory accessible to an ISE admin client.

Importing the Library

Access the ISE admin interface and navigate to **Policy > Profiling > Profiling Policies** and select **Import** from the right-hand menu.

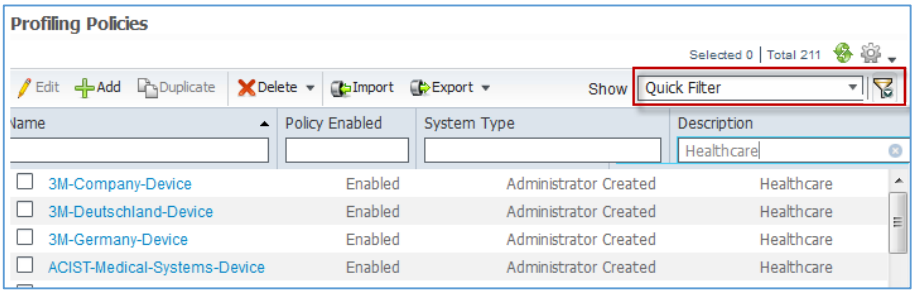


Click **Browse** and select the downloaded file and click **Submit** to begin the import process.



A pop-up window will indicate the progress of the import. When it's completed, click **Ok** to acknowledge completion of the import.

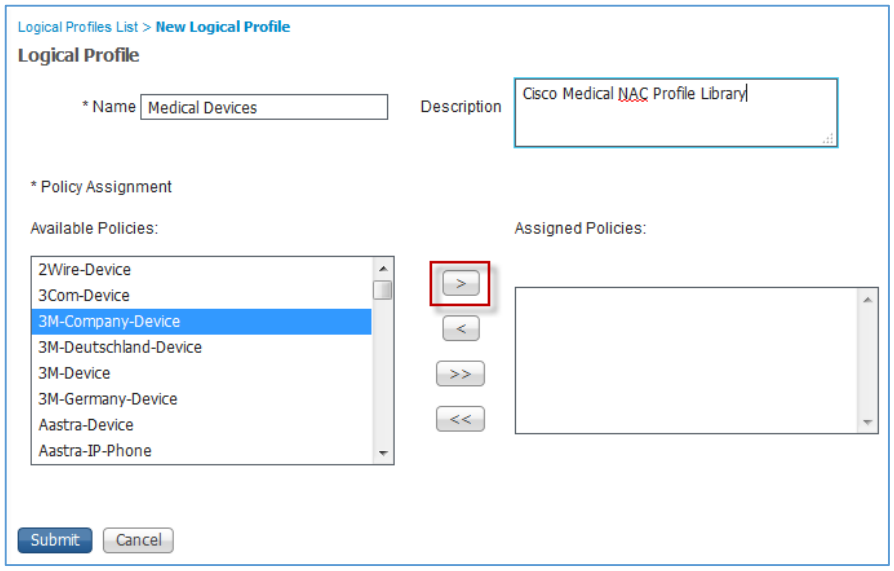
To verify the import, select the **Filter** icon and enter “Healthcare” in the Description field:



Establish Logical Groups

Logical groups are a way to put endpoints together based on their endpoint profile. All endpoints that match one of the child profiles can then be viewed in one logical group. Additionally, an authorization policy can be applied to logical groups.

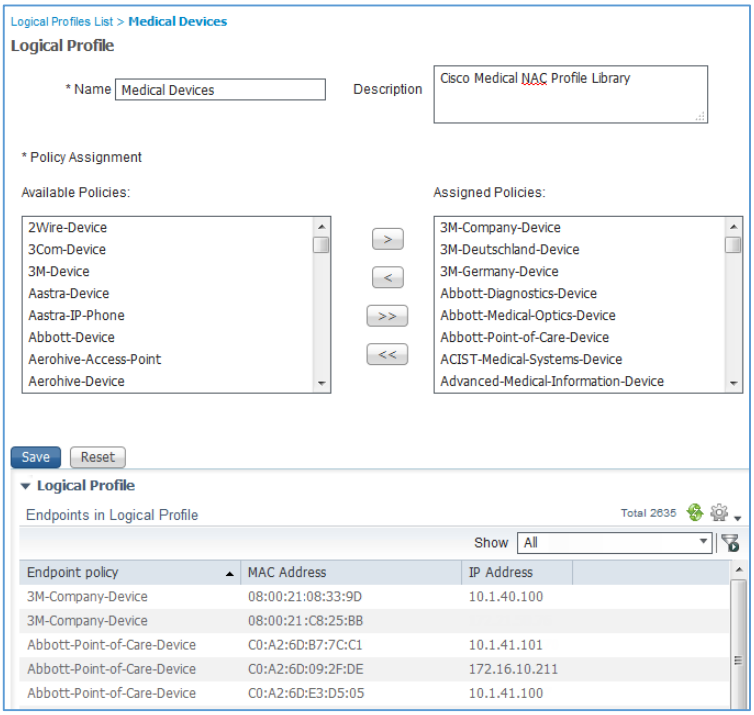
Now that you have imported the Cisco Medical NAC Profile Library, it may be useful to add its devices to a logical group. To complete this task, navigate to **Policy > Profiling > Logical Profiles** from the ISE Admin interface. Click **Add** and enter a name for the Logical Profile, for example “Medical Devices” and an optional description.



Select the appropriate profiles from the Available Policies list on the left. Use the > arrow key to move the selected policies to the Assigned Policies list on the right.

The Shift key can be used to select a range of sequential entries. On Windows, the Control (Ctrl) key can be used to select multiple nonsequential entries.

When complete, click **Save**. A list of all matching endpoints is displayed.



Depending on organizational and policy requirements, it may be necessary to create multiple logical profiles to group the medical devices by function, type, or department. Profiler policies, and thus endpoints, may belong to multiple logical profiles.

Segmentation

Overview

Once endpoints have been discovered, classified (profiled), and optionally assigned to one or more logical profiles, ISE can use this information to make a more informed policy decision. Actual policy will require careful consideration of the security risks as well as the potential impact to endpoint connectivity. Many healthcare providers are faced with the challenge that they are not aware of all medical devices and their traffic requirements. Attempts to segment or limit network access may result in a service disruption that may pose a risk to a patient's health, a risk that outweighs the security risk.

The possibility that service may be denied to legitimate medical devices and their supporting systems leads many healthcare IT administrators to opt for a monitor-only policy, at least until the environment is better understood.

Segmentation Using Dedicated Networks

A traditional method for segmenting medical devices is to completely isolate them in one or more dedicated networks. Although intuitive and straightforward, this method is diminishing in popularity because of the cost of managing separate networks. These networks often require integration with shared resources and partner networks, which makes controlled separation and "leakage" difficult to manage. Furthermore, the dedication of

physical ports restrictsthe mobility of devices and carts that require ports to be available at any location. Some providers have reported that they were unable to use certain critical devices in different hospital rooms. A room may have been available, but the dedicated network ports were not.

For wireless devices it is also possible to deploy a dedicated network of access points and controllers. But again, the cost of managing separate systems with redundancy is extremely costly and may result in interference between wireless networks. For these reasons, healthcare delivery organizations commonly opt for a shared infrastructure with virtual segmentation.

Segmentation Using ACLs

The use of access control lists (ACLs) to limit or segment traffic may be preferred when the allowed ports and destinations are well known. A benefit of ACLs is that they can limit or eliminate the need for virtual local area networks (VLANs) to separate endpoint traffic.

One challenge with ACLs is the need to manage the lists on the access devices. Cisco supports downloadable ACLs (dACLs), which allow ACLs to be centrally managed, but maintaining these policies can still be cumbersome, especially if they change frequently. Another challenge with ACL enforcement is that they are intended for access policy to be roughly defined. In other words, hardware limits often restrict the number of ACL rules on the access device to a few entries. Firewalls are typically required to provide more granular policy control further upstream in the network or closer to the protected hosts.

To implement a monitor-only policy for medical devices, ISE can assign an ACL that permits all access (for example, “permit ip any any”).

Segmentation Using VLANs and WLANs

VLANs and wireless LANs (WLANs) are commonly used to segment medical networks. A key advantage of VLANs is that they are intuitive. All the devices in the same VLAN are virtually segmented from the devices in other VLANs. However, VLANs do not guarantee traffic separation. Unless VLANs are completely isolated through the use of virtual routing and forwarding (VRF) or a similar method, ACLs or other firewall services are needed at the VLAN boundaries.

A major challenge using VLANs for network segmentation is the need to define and coordinate the assignment of these separate networks across the access layer. IP address management also becomes more difficult because each VLAN must typically be assigned its own subnetwork. Finally, DHCP may not work as expected if the endpoint is allowed to acquire an IP address in an initial VLAN and is then assigned a different VLAN upon authorization. Some hosts can detect this VLAN change while others do not. In the latter case, the endpoint may be stuck without access due to an IP mismatch.

To implement a monitor-only policy for medical devices, ISE can assign a VLAN that segregates the Layer 2 traffic but does not restrict IP access.

Note: A VLAN-based policy requires that static endpoints have been assigned an appropriate IP address for the authorized VLAN. DHCP-enabled medical devices may require “closed mode” port authentication, whereby a VLAN is assigned only after authentication to avoid the case where the host acquires an initial VLAN IP address.

Cisco TrustSec Technology and pxGrid

Also growing in popularity is the Cisco TrustSec software-defined segmentation method. This segmentation uses logical tags known as security group tags, or SGTs. At the point of network authorization, Cisco ISE can “mark” or tag matching endpoints as critical medical devices without changing its VLAN or assigning a specific IP address. Although they are compatible with traditional segmentation methods, SGTs can eliminate the need for VLAN proliferation or port ACLs. SGTs can be used purely for visibility or policy enforcement virtually anywhere in the network. Firewalls that support Cisco TrustSec technology can dynamically apply policy without concern over source IP or VLAN assignment, which simplifies rule management. Unlike ACLs and VLANs, Cisco TrustSec segmentation is independent from the network topology and topology changes.

In the context of medical devices, SGTs offer an attractive option. You can use them to track and monitor medical devices without applying enforcement and later apply more restrictive segmentation and access to and from these devices. These policy markings are also made available to external applications through Cisco pxGrid, a framework for data sharing. Cisco pxGrid greatly enhances visibility and policy compliance validation for critical-care and other healthcare systems using solutions such as Cisco Stealthwatch and the Cisco Firepower™ Management Center as well as Splunk and a host of other third-party ecosystem partners. For more information on Cisco ISE partners that support pxGrid, see http://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/solution-overview-c22-735909.html.

SGT Authorization Policy Example

The example policy rules below show the use of logical profiles to match medical devices on a wired network to assign a permissions policy that permits access and marks the endpoint as a healthcare endpoint using a security group tag labeled “Healthcare.”

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wired Medical Devices	if	(Wired_MAB AND EndPoints:LogicalProfile EQUALS Medical Devices)	then	PermitAccess AND Healthcare

APPENDIX A—Medical Device Custom Profile Checklist

If existing profiles fail to identify specific medical devices, it may be necessary to define custom profiles. This checklist can be used to determine the primary characteristics of the endpoint that can aid in classifying and creating custom profiles.

The form asks a series of questions that aim to help you understand what types of information may be available from the device and which probes should be used to collect the relevant information. This process helps focus profiling efforts on methods that are more likely to yield useful results. It can also highlight potential gaps in profiling or opportunities for successful classification.

Once the main attributes are understood, a custom profile can be generated from the form. Each unique device model or type will have its own record.

Device Characteristics				
	Vendor	Ex: Draeger		
	• Vendor contact info			
	• Vendor webpage			
	Device	Ex: Delta		
	Model			
	Device type, function, or category	Ex: Patient Monitor		
	Wired or wireless	Ex: Wired		
	Typical supported platform	Appliance or whitebox?		
	• NIC vendor (= OUI)	Specific vendor(s) or any?		
	• OS type and version	Windows? Linux? Other?		
	• Hardened OS?			
	Can authenticate: Yes/No			
	• 802.1X or EAP			
	• Protocol (PEAP, TLS, PSK)			
	IP addressing (DHCP)			
	• Static IP: Yes/No	Yes		
	• Static DHCP: Yes/No	No		
	• DHCP user class ID configurable: Yes/No			
	Host/DNS Naming (DNS/DHCP)			
	• Hostname: static or configurable			

Device Characteristics				
	• Follow naming standard: Yes/No			
	LLDP or CDP capable (SNMP): Yes/No			
	Scans allowed (Nmap): Yes/No			
	SNMP manageable (Nmap): Yes/No			
	Web capable (HTTP): Yes/No			
	Predictable traffic flows (NetFlow): Yes/No	Yes		
	Source IP or range	Ex: 224.127.1.x-254		
	Source port or range	Ex: 2150		
	Destination IP or range	Ex: 192.168.100.y, 192.168.200.z		
	Destination port or range	Ex: 2150		
	Protocol(s)	Ex: UDP 17		
Probe	**Attribute**	**Value**	**Possible Values**	**Notes**
RADIUS, SNMP, DHCP	MAC address	Ex: 00:30:e6:01:ea:3f		
	OUI	Ex: Draeger Medical Systems Inc		
RADIUS, SNMP, DHCP	IP Address	Ex: 224.127.1.253	224 127 MU 252 , 224 127 MU 253, 224 127 MU 254, 224 127 MU 255, 224 127 MU X	MU = monitoring unit
DNS	FQDN	Ex: MU1239532.cardio.hospital.com		MU = monitoring unit
DHCP	client-fqdn	Ex: MU1239532.cardio.hospital.com		MU = monitoring unit
	host-name	Ex: MU1239532		MU = monitoring unit
	dhcp-user-class-identifier			
	dhcp-class-identifier			
	dhcp-parameter-request-list			
NetFlow	IPV4_SRC_ADDR	Ex: 224.127.1.x-254		
	L4_SRC_PORT	Ex: 2150		
	IPV4_DST_ADDR	Ex: 192.168.100.y, 192.168.200.z		
	L4_DST_PORT	Ex: 2150		
	PROTOCOL	Ex: UDP 17		
HTTP	User-Agent			
Nmap	operating-system			
	xxx-tcp			
	yyy-udp			
Nmap-SNMP	sysName			
	sysDescr			
	sysContact			

Device Characteristics				
	sysLocation			
	hrDeviceDescr			
SNMP-LLDP	lldpCapabilitiesMapSupported			
	lldpChassisId			
	lldpSystemName			
	lldpSystemDescription			
SNMP-CDP	cdpCacheCapabilities			
	cdpCacheDeviceId			
	cdpCachePlatform			
	cdpCacheVersion			

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-737205-00 05/16