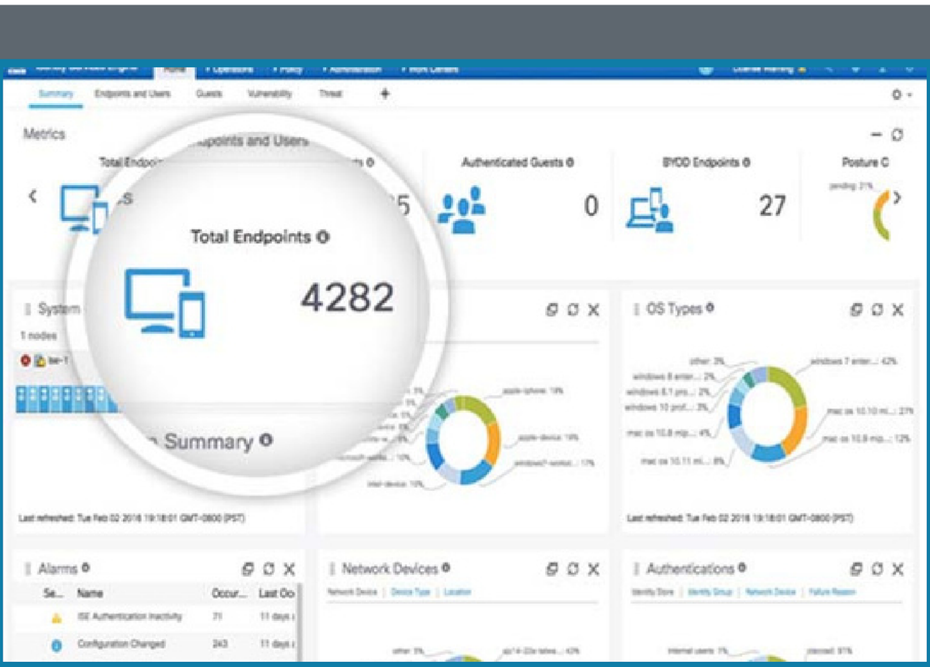
accendnetworks®



Security

Cisco ISE

Part II- 802.1x Auth/AuthZ, ISE Profiling Probes, Posturing, WLAN Dot1X, TrustSec, and Troubleshooting.

Paula Wong, CEO/Founder, CCIE#13062
Senior Security Architect/Network Engineer

TABLE of Contents

1 INTRODUCTION

2 CHAPTER 1 – 802.1x Authentication/Authorization

3 CHAPTER 2 – Cisco ISE Profiling Services

4 CHAPTER 3 – Cisco ISE Posturing

5 CHAPTER 4 – WLAN Dot1x Deployment

6 CHAPTER 5 – WLAN Access Control

7 CHAPTER 6 - Segmentation using Cisco TrustSec

8 CHAPTER 7 - ISE Troubleshooting

9 CHAPTER 8 - CONTACT US!

CHAPTER - 1

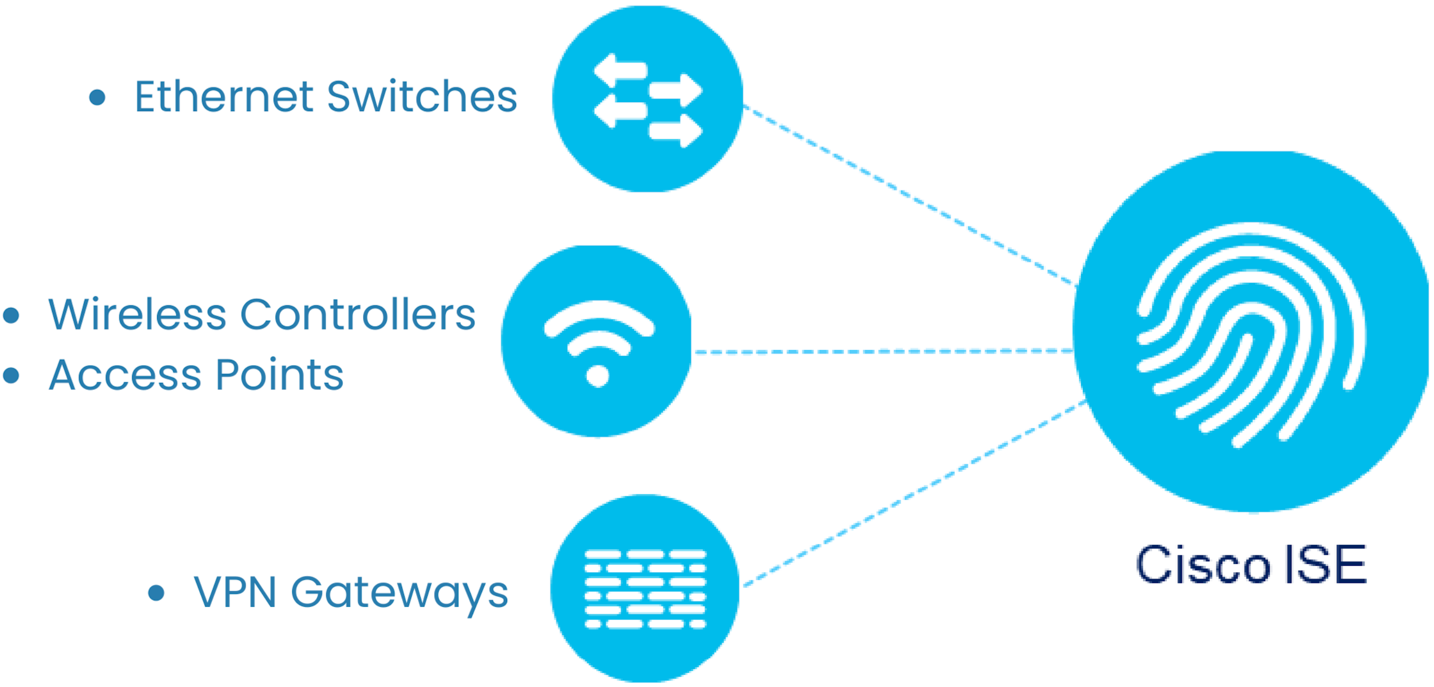
802.1x Auth/AuthZ

CISCO IDENTITY SERVICES ENGINE (ISE)

Delivers Network Access Control (NAC)

- RADIUS Server
- TACACS+ Server

(OR NETWORK ACCESS DEVICES = NAD)



- Ethernet Switches
- Wireless Controllers
- Access Points
- VPN Gateways

Cisco ISE

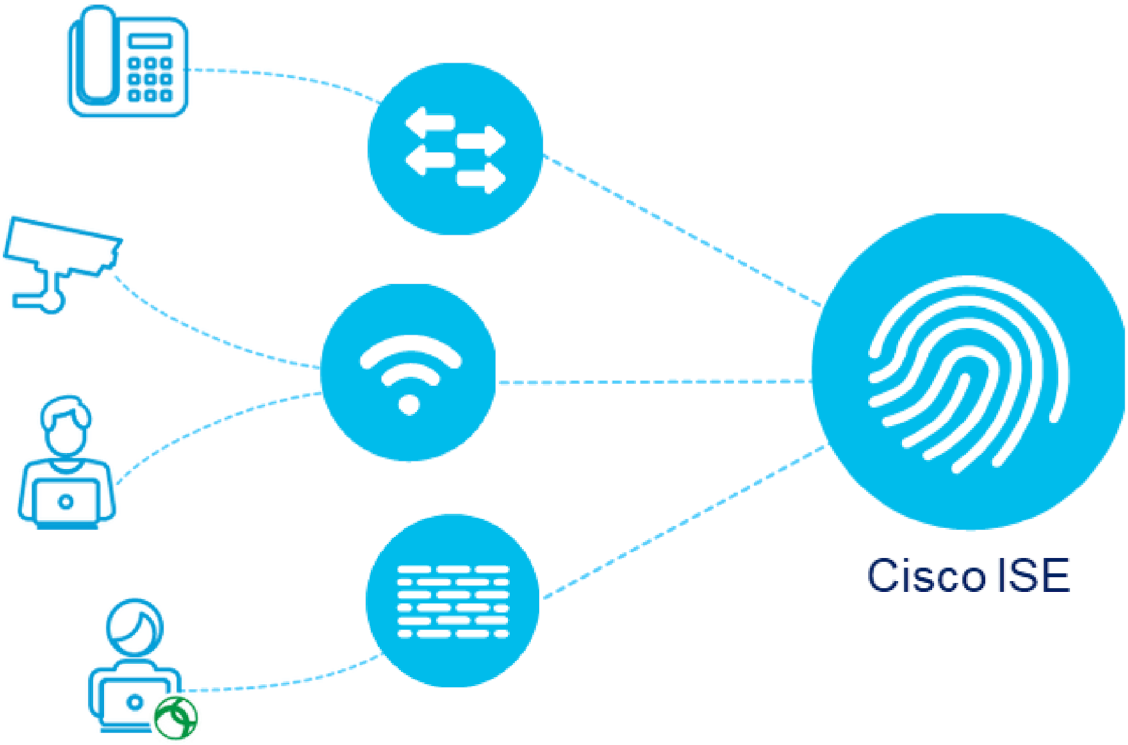
Network Access by

Network Devices

USERS AND ENDPOINTS

WITH VALID CREDENTIALS, ENDPOINTS GET CONTROLLED ACCESS

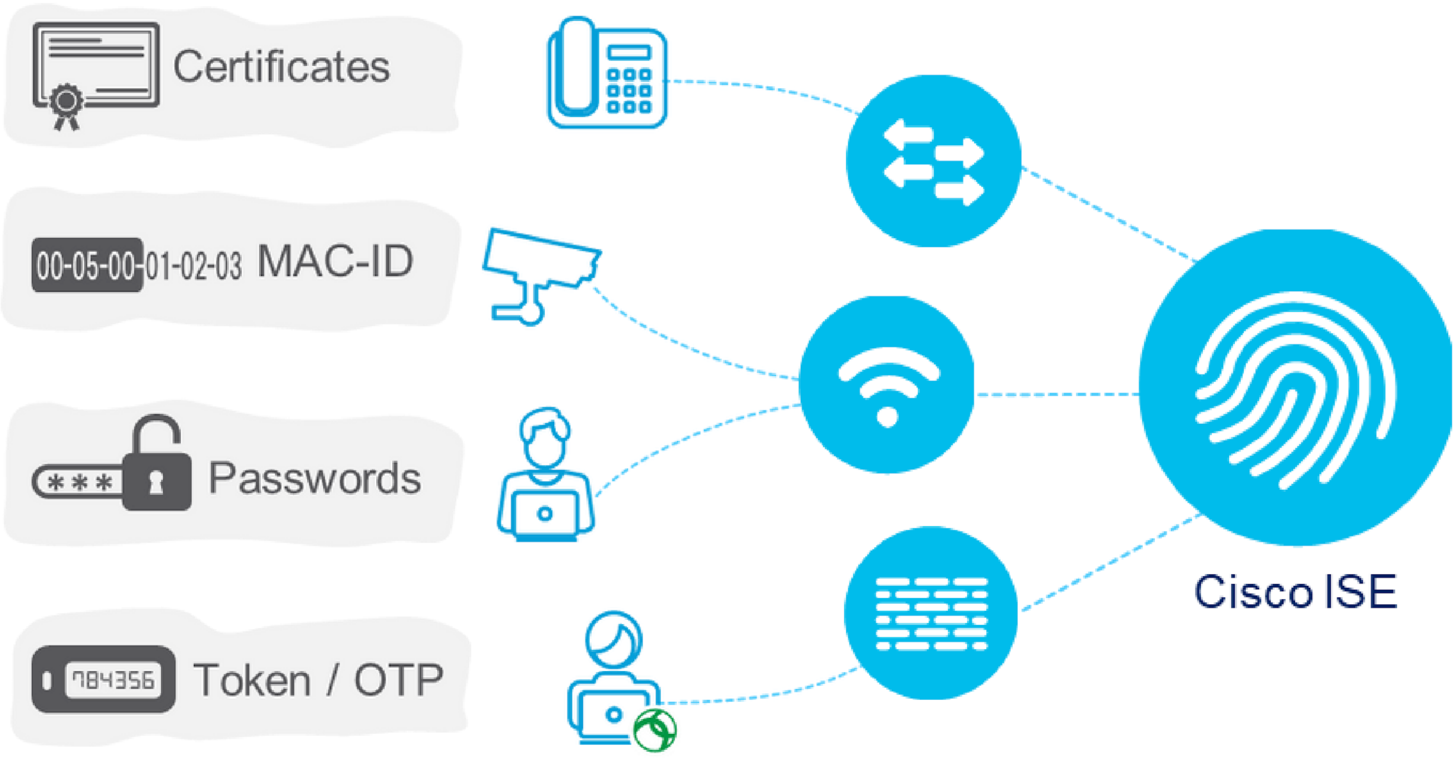
- Users
- IP Phones
- Printers
- Camera
- Things
- and more



Network Access for

Endpoints

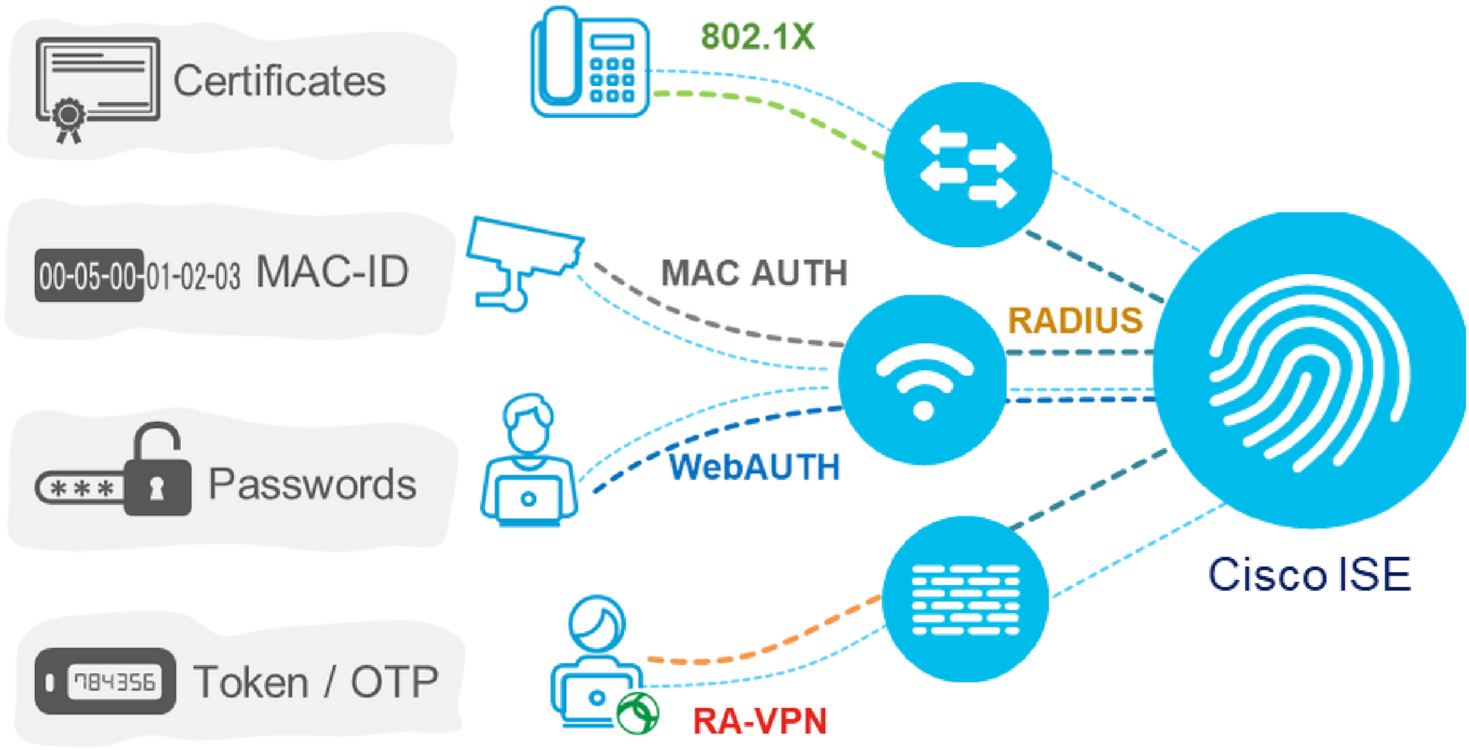
CREDENTIALS



Identify Endpoints by

Credentials

AUTHENTICATION

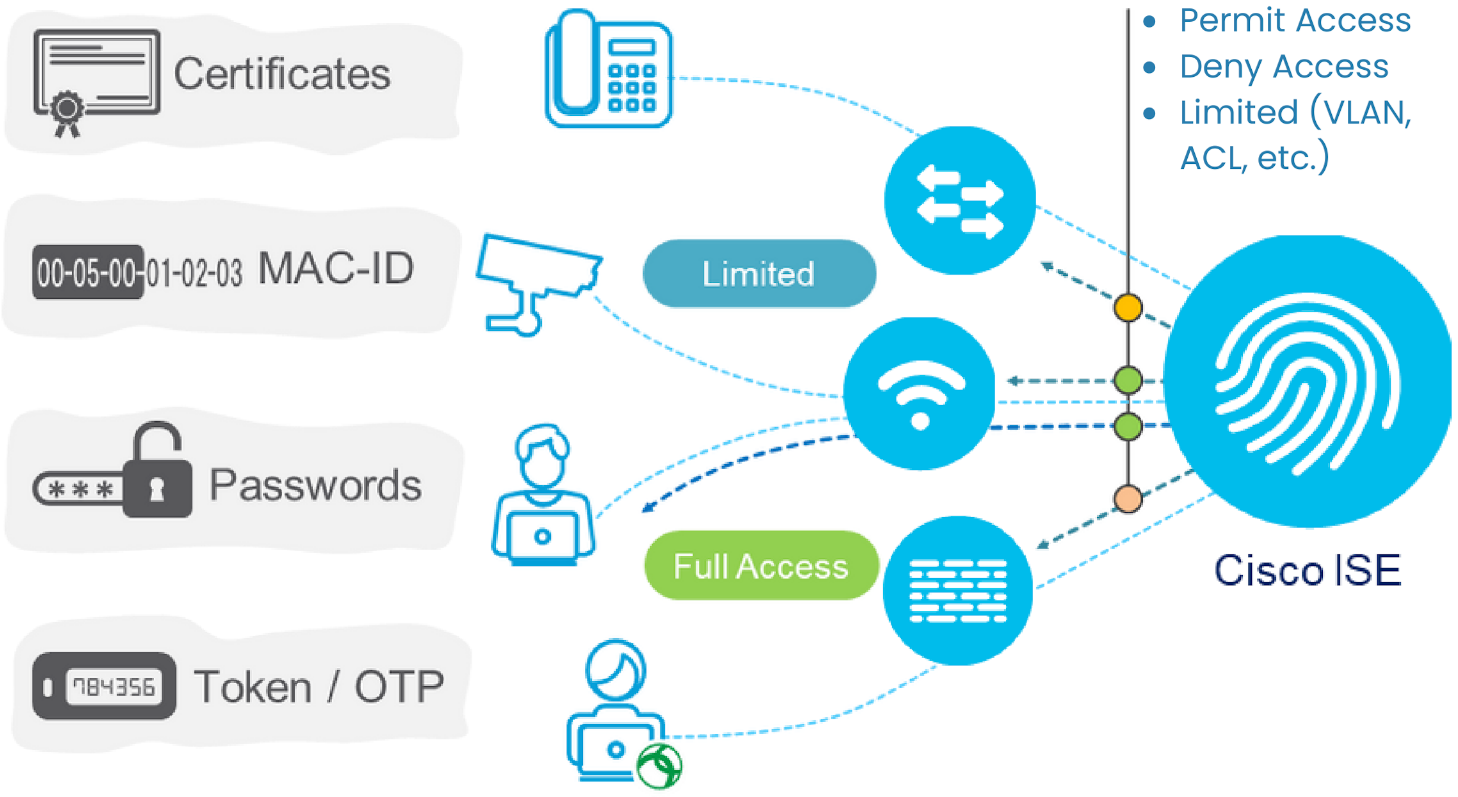


Credentials passed to ISE by

Authentication

You tell ISE who you are

AUTHORIZATION



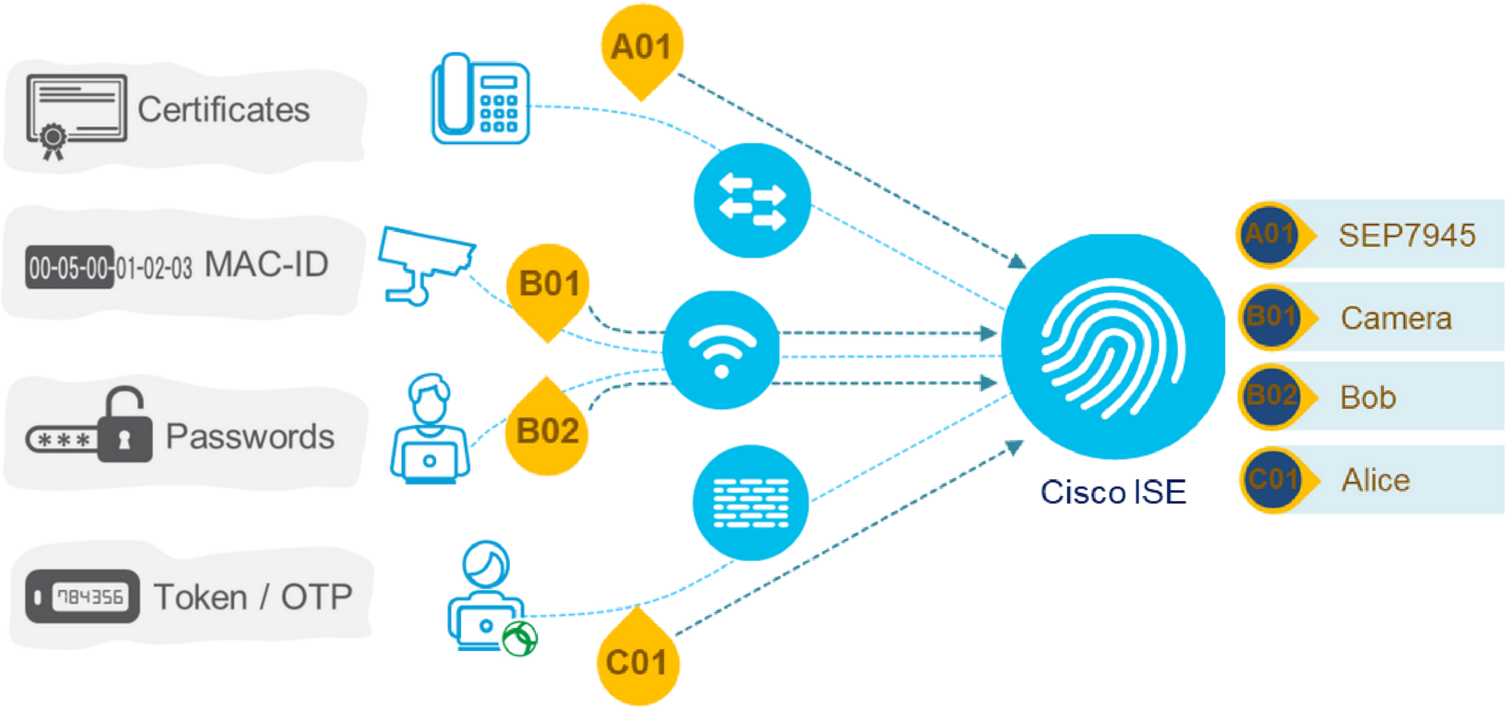
Authentication results in

Authorization

ISE tells network, your level of access

SESSIONS AND SESSION-ID (IDENTIFIER)

SESSION AWARE NETWORKING

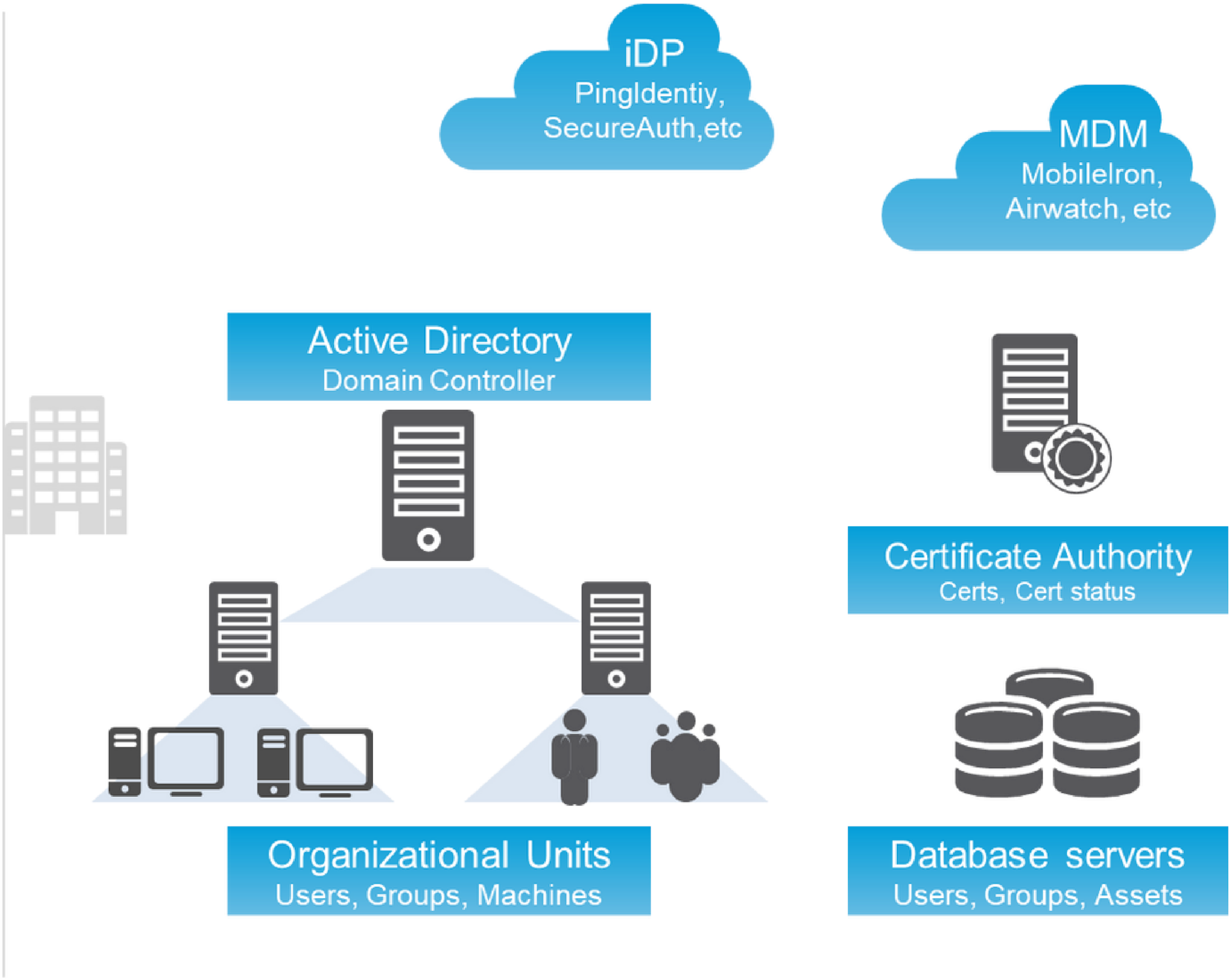


Track endpoint's network association by

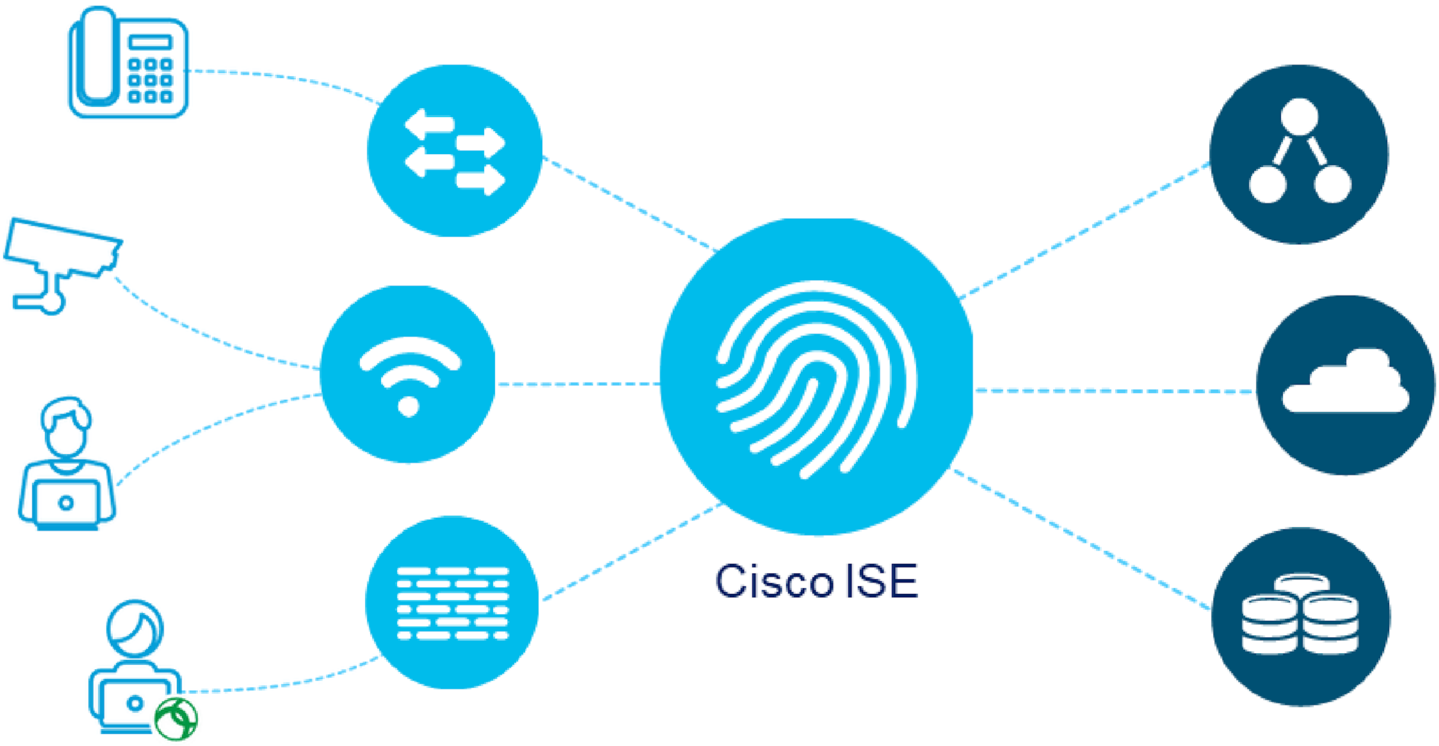
Session-ID

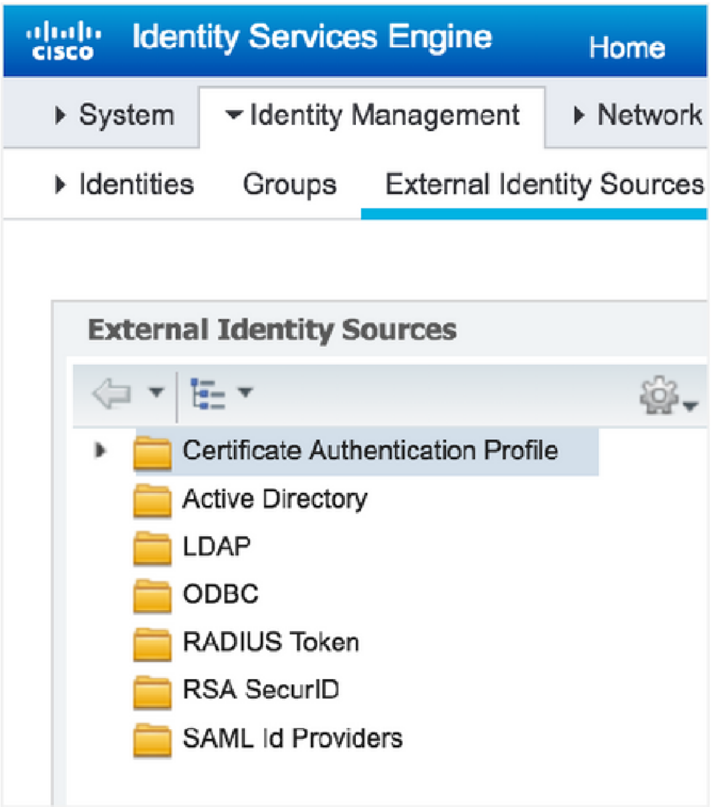
SOMETHINGS ALREADY EXIST

A typical environment already has a bunch of services which ISE can leverage by integrating seamlessly



IDENTITY STORE INTEGRATIONS





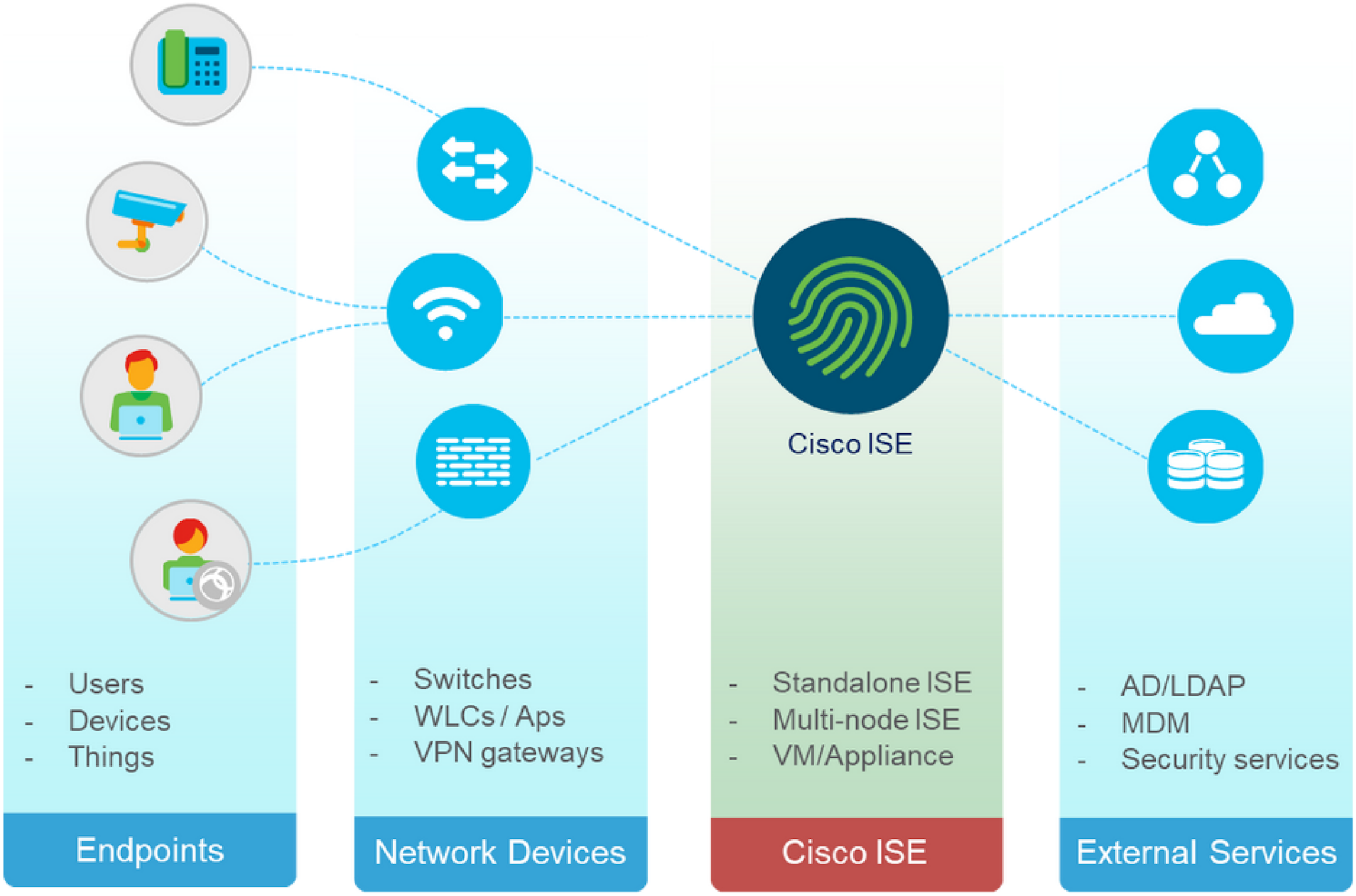
External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers

Validate Endpoints via

External Identity Sources

WHAT MAKES UP AN ISE DEPLOYMENT?



- Users
- Devices
- Things

Endpoints

- Switches
- WLCs / Aps
- VPN gateways

Network Devices

- Standalone ISE
- Multi-node ISE
- VM/Appliance

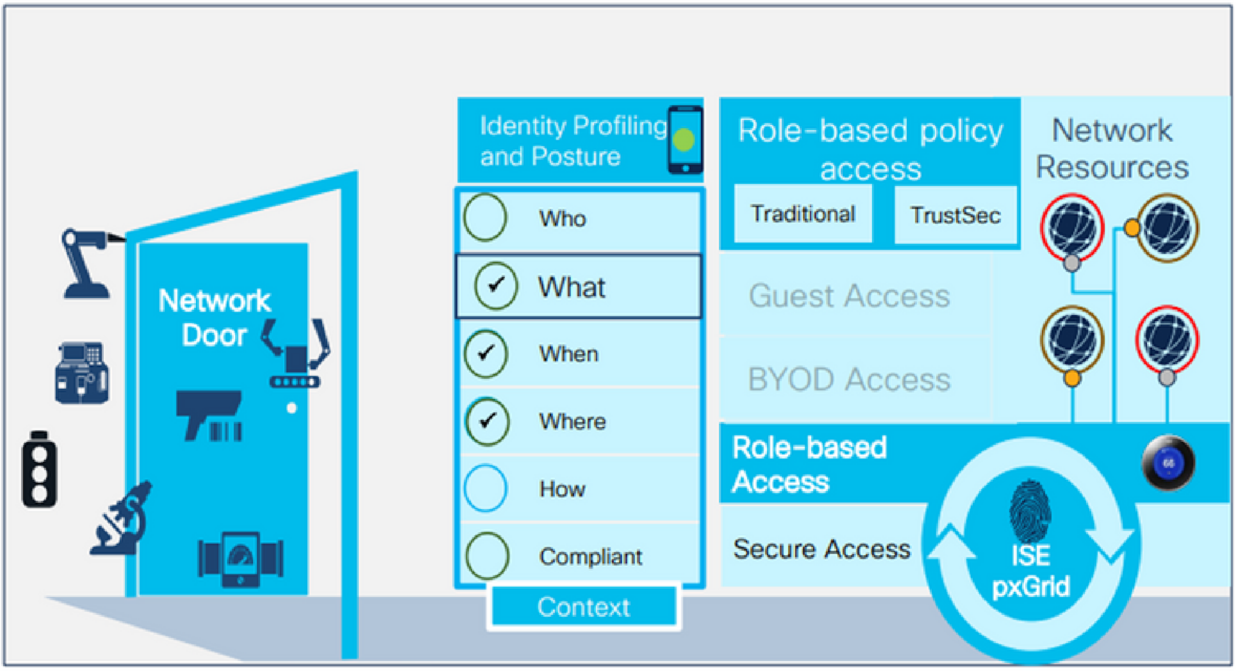
Cisco ISE

- AD/LDAP
- MDM
- Security services

External Services

2. CISCO ISE PROFILING SERVICES

ENDPOINT VISIBILITY BASED ON CONTEXT CISCO IDENTITY SERVICES ENGINE (ISE)



ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							

ISE data collection methods for Device profiling

Context information allows implementation of the Principle of Least Privilege

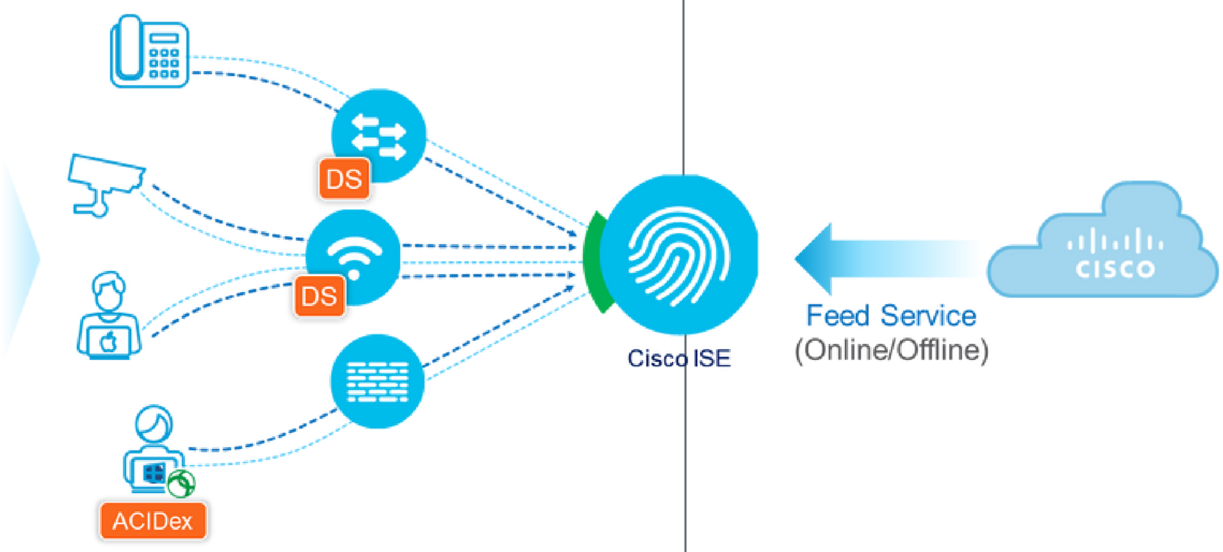
- Infusion Pump
- Vendor
- Building-A Floor-1
- 10:30 AM EST on April 27
- Wireless / Ethernet / Zigbee
- No Threats / Vulnerabilities

VISIBILITY DATA SOURCES

ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							

ISE data collection methods for Device profiling

Endpoints send interesting data, that reveal their device identity



Profiler Policy

If CDP:Platform Name = **Cisco IP Phone** = true, then Cisco-IP-Phone

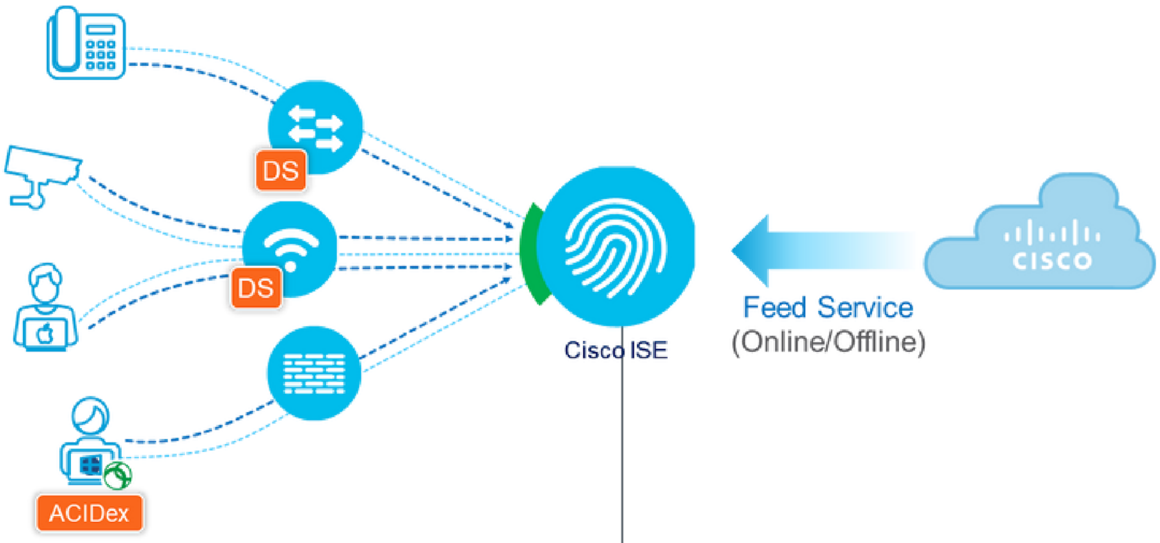
Authorization Policy

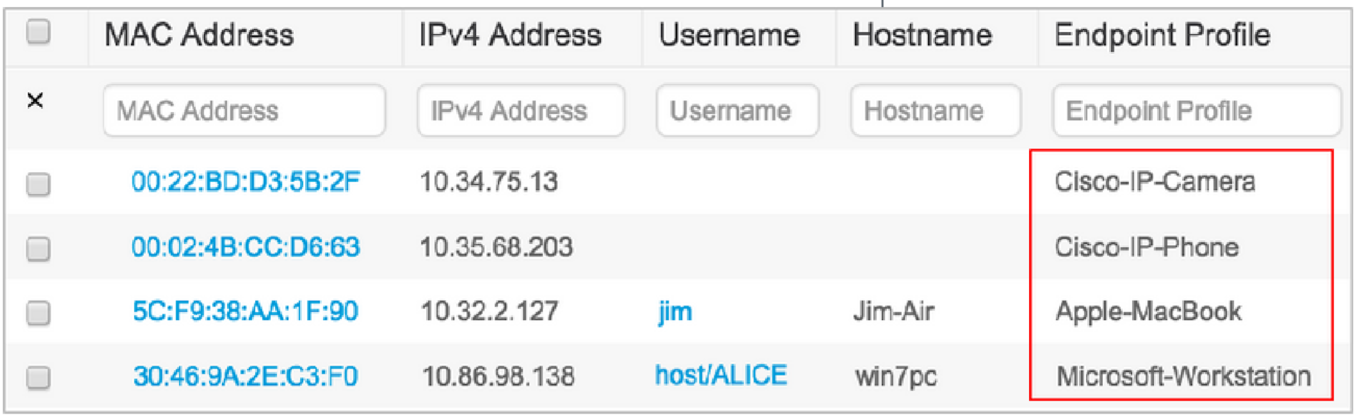
If Endpoint ID Group = Cisco-IP-Phone = true, then Voice VLAN

AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

VISIBILITY DATA SOURCES

Endpoints send interesting data, that reveal their device identity

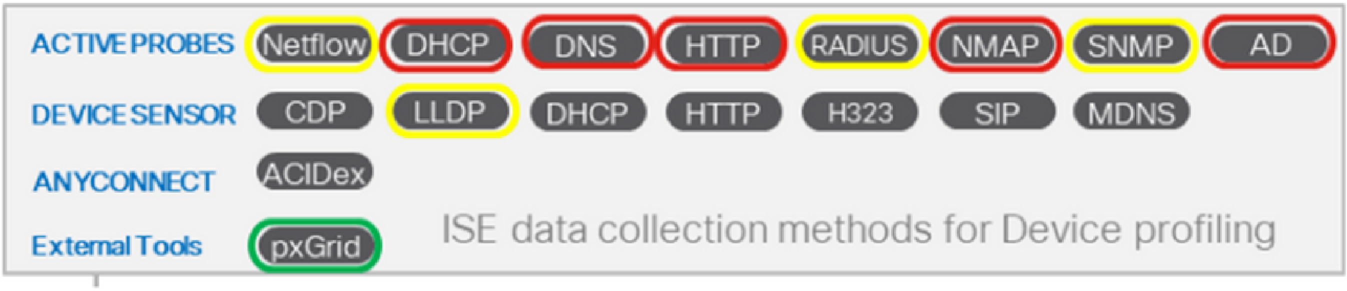




□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
□	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
□	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
□	30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

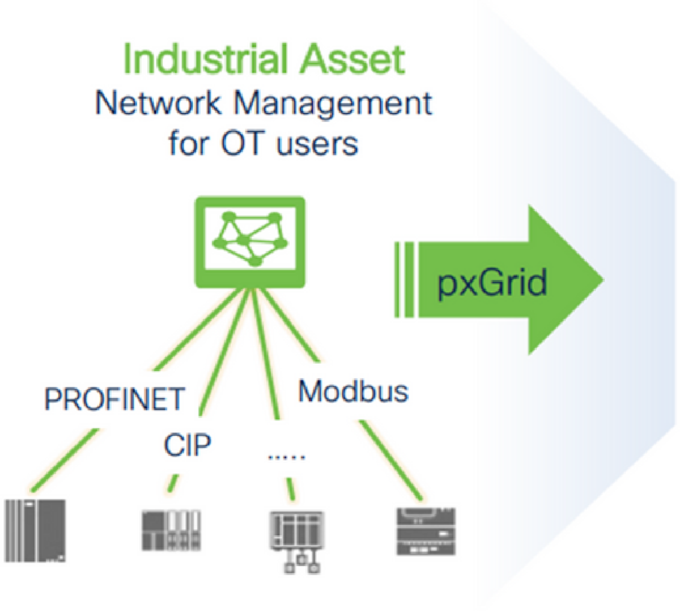
AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

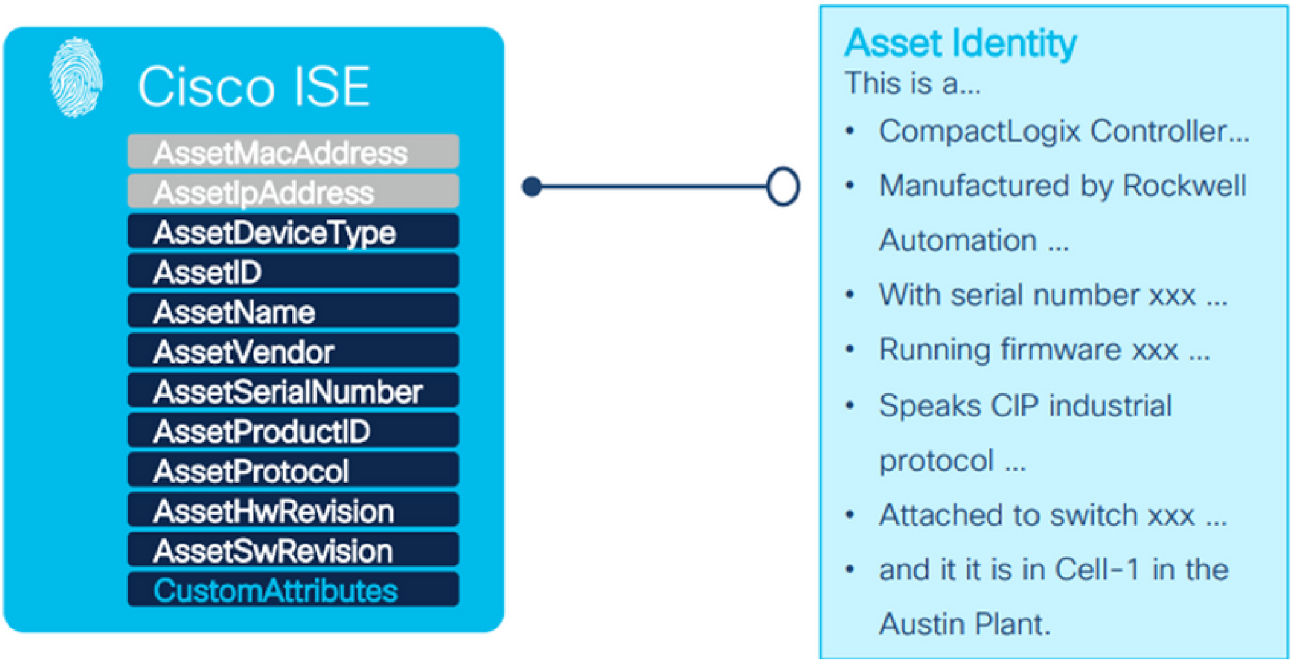
SHARING INDUSTRIAL ASSET WITH ISE RECOMMENDED PROFILING PROBES



ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							
External Tools	pxGrid							

ISE data collection methods for Device profiling





Cisco ISE

- AssetMacAddress
- AssetIpAddress
- AssetDeviceType
- AssetID
- AssetName
- AssetVendor
- AssetSerialNumber
- AssetProductID
- AssetProtocol
- AssetHwRevision
- AssetSwRevision
- CustomAttributes

Asset Identity

This is a...

- CompactLogix Controller...
- Manufactured by Rockwell Automation ...
- With serial number xxx ...
- Running firmware xxx ...
- Speaks CIP industrial protocol ...
- Attached to switch xxx ...
- and it it is in Cell-1 in the Austin Plant.