cisco Partner
Distribution Partner

ЛАН СИСТЕМС

MUK
Classics of distribution

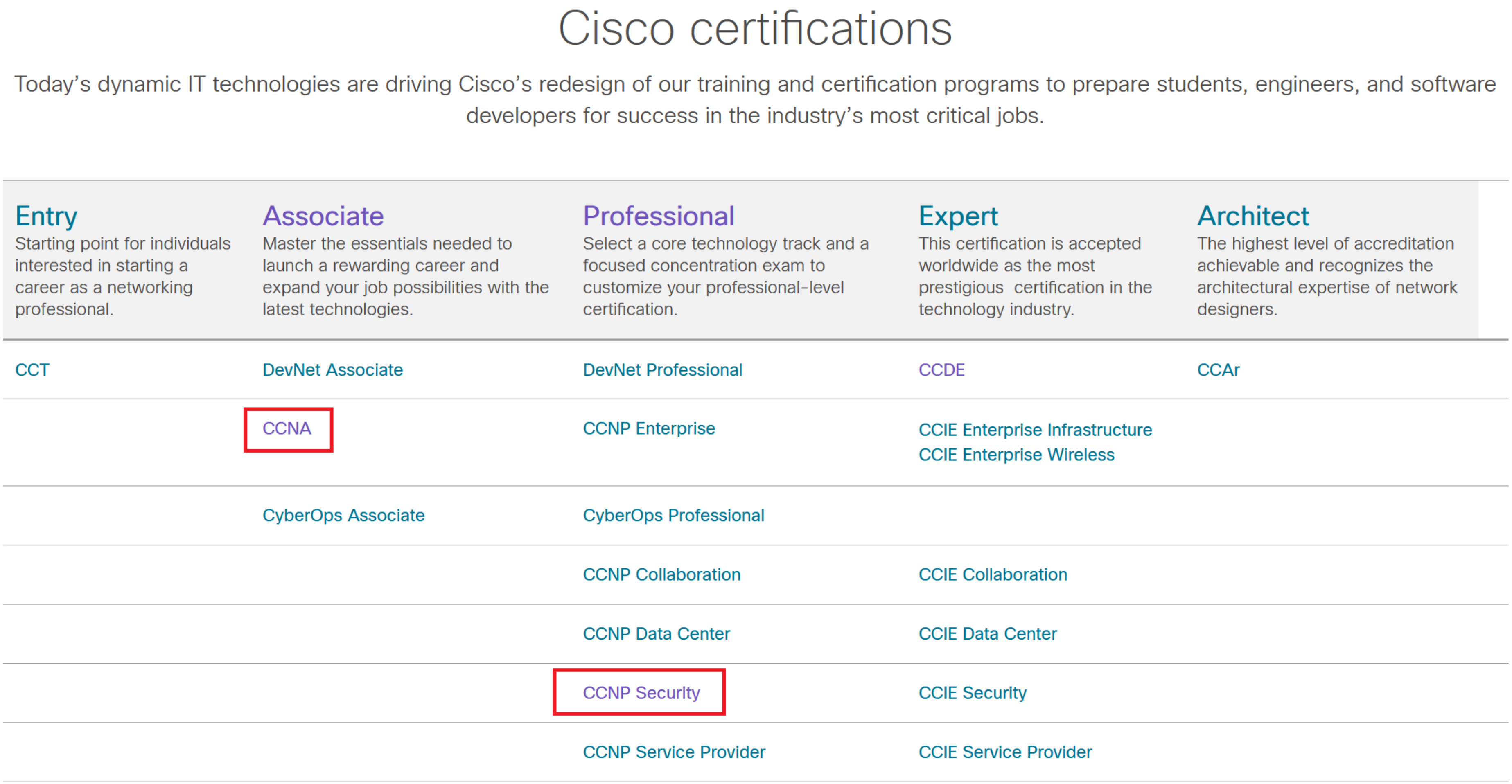
Использование Cisco ISE в эпоху «нулевого доверия» Zero Trust для сетей, приложений и рабочей среды

Security

Сергей ГАЩЕНКО

sha@lansys.com.ua

19.01.2021

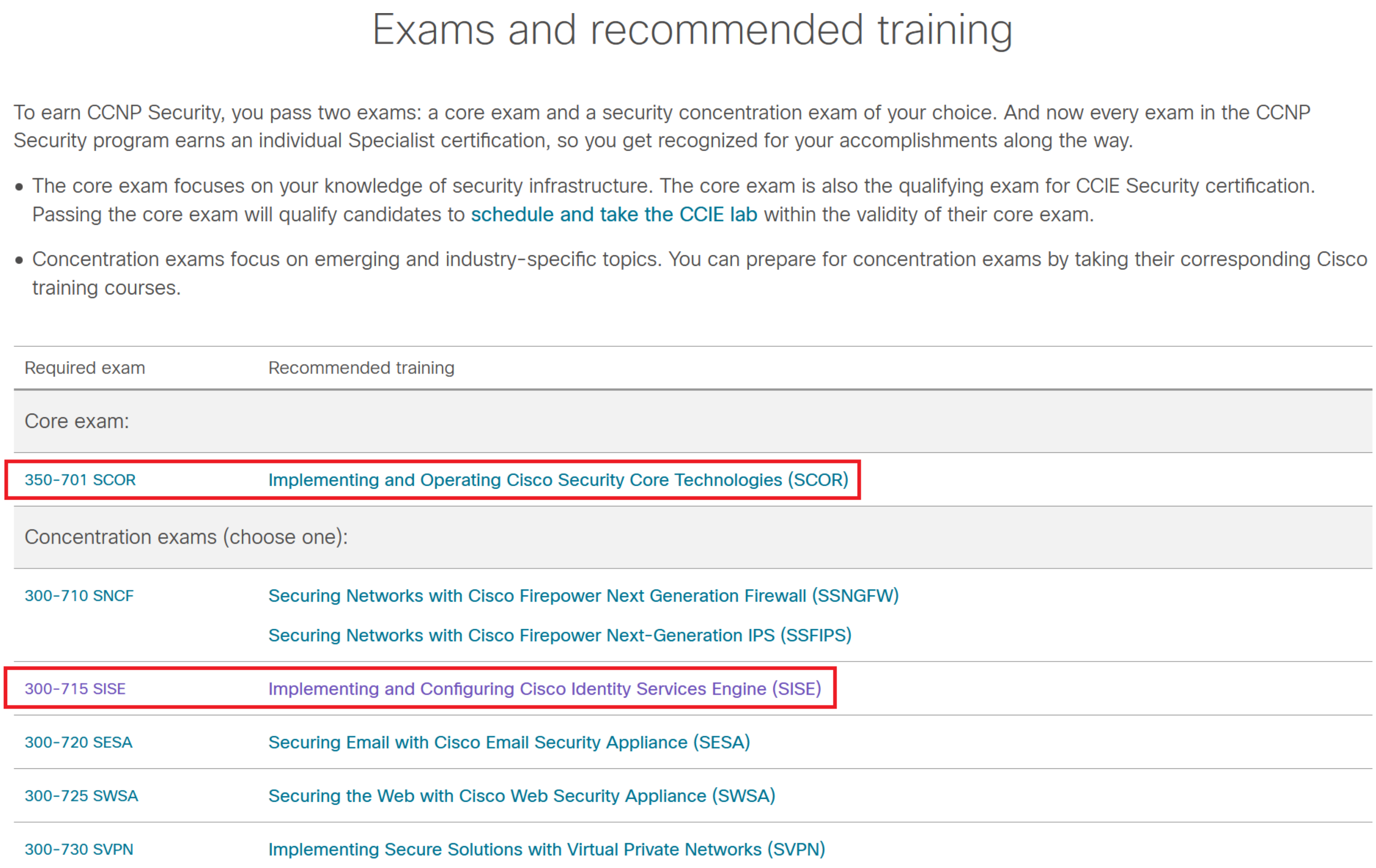


Cisco certifications

Today's dynamic IT technologies are driving Cisco's redesign of our training and certification programs to prepare students, engineers, and software developers for success in the industry's most critical jobs.

Entry	Associate	Professional	Expert	Architect
Starting point for individuals interested in starting a career as a networking professional.	Master the essentials needed to launch a rewarding career and expand your job possibilities with the latest technologies.	Select a core technology track and a focused concentration exam to customize your professional-level certification.	This certification is accepted worldwide as the most prestigious certification in the technology industry.	The highest level of accreditation achievable and recognizes the architectural expertise of network designers.
CCT	DevNet Associate	DevNet Professional	CCDE	CCAr
	CCNA	CCNP Enterprise	CCIE Enterprise Infrastructure CCIE Enterprise Wireless	
	CyberOps Associate	CyberOps Professional		
		CCNP Collaboration	CCIE Collaboration	
		CCNP Data Center	CCIE Data Center	
		CCNP Security	CCIE Security	
		CCNP Service Provider	CCIE Service Provider	

cisco.com/go/certifications

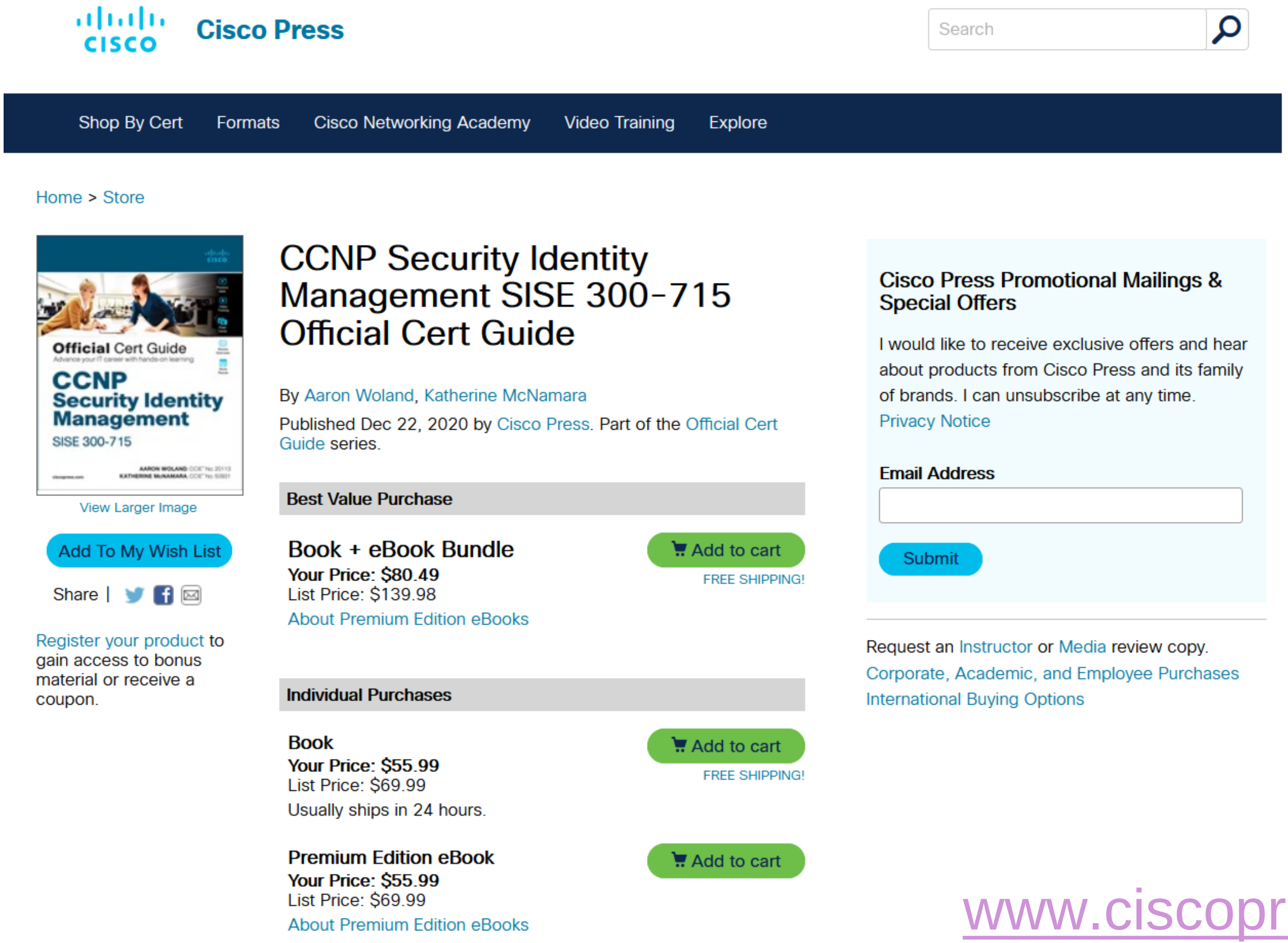


Exams and recommended training

To earn CCNP Security, you pass two exams: a core exam and a security concentration exam of your choice. And now every exam in the CCNP Security program earns an individual Specialist certification, so you get recognized for your accomplishments along the way.

- The core exam focuses on your knowledge of security infrastructure. The core exam is also the qualifying exam for CCIE Security certification. Passing the core exam will qualify candidates to schedule and take the CCIE lab within the validity of their core exam.
- Concentration exams focus on emerging and industry-specific topics. You can prepare for concentration exams by taking their corresponding Cisco training courses.

Required exam	Recommended training
Core exam:	
350-701 SCOR	Implementing and Operating Cisco Security Core Technologies (SCOR)
Concentration exams (choose one):	
300-710 SNCF	Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW) Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)
300-715 SISE	Implementing and Configuring Cisco Identity Services Engine (SISE)
300-720 SESA	Securing Email with Cisco Email Security Appliance (SESA)
300-725 SWSA	Securing the Web with Cisco Web Security Appliance (SWSA)
300-730 SVPN	Implementing Secure Solutions with Virtual Private Networks (SVPN)



CCNP Security Identity Management SISE 300-715 Official Cert Guide

By Aaron Woland, Katherine McNamara

Published Dec 22, 2020 by Cisco Press. Part of the Official Cert Guide series.

Register your product to gain access to bonus material or receive a coupon.

Best Value Purchase

Book + eBook Bundle
Your Price: $80.49
List Price: $139.98
About Premium Edition eBooks
FREE SHIPPING!

Individual Purchases

Book
Your Price: $55.99
List Price: $69.99
Usually ships in 24 hours.
FREE SHIPPING!

Premium Edition eBook
Your Price: $55.99
List Price: $69.99
About Premium Edition eBooks

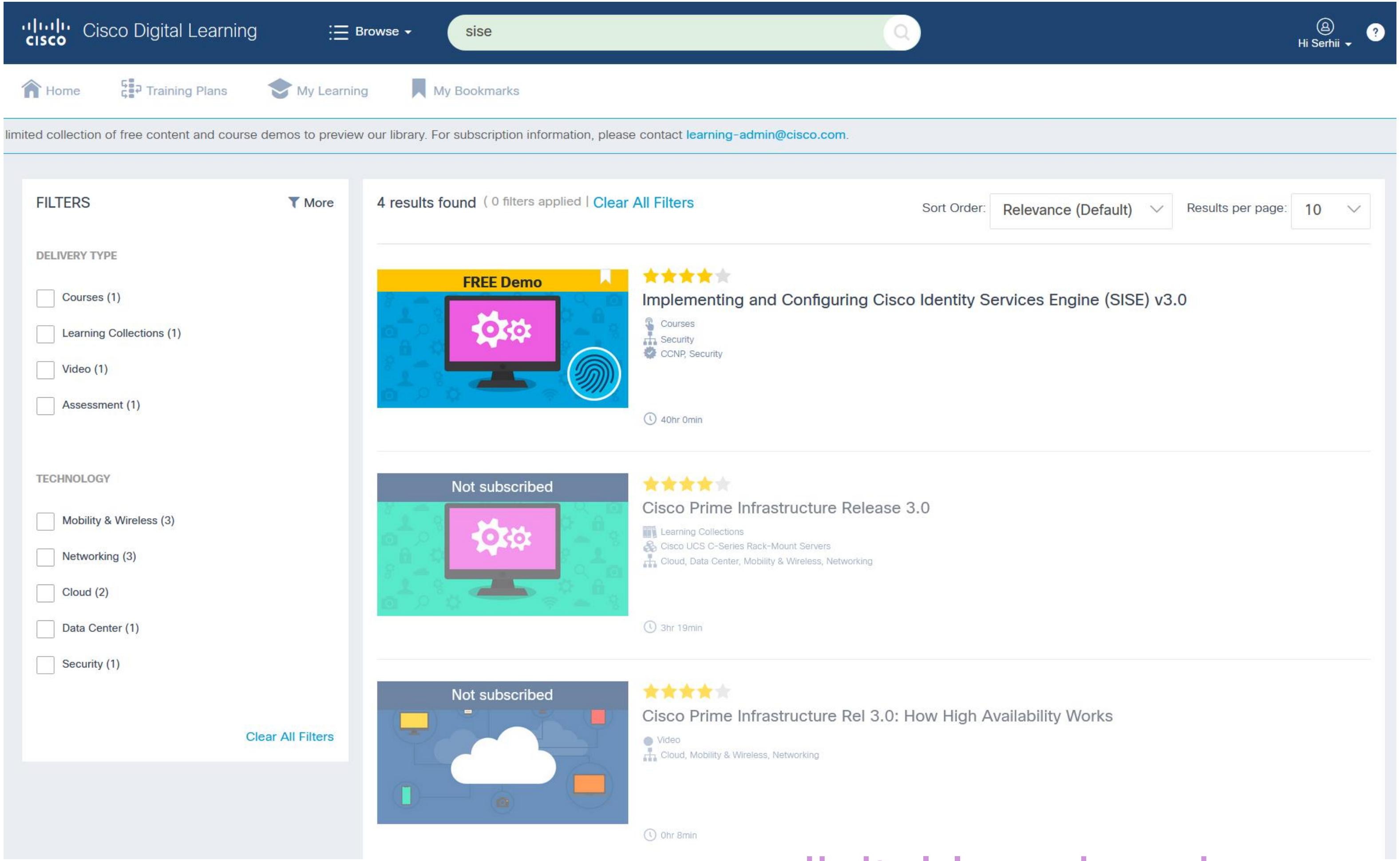
Cisco Press Promotional Mailings & Special Offers

I would like to receive exclusive offers and hear about products from Cisco Press and its family of brands. I can unsubscribe at any time. Privacy Notice

Email Address

Request an Instructor or Media review copy.
Corporate, Academic, and Employee Purchases
International Buying Options

www.ciscopress.com



limited collection of free content and course demos to preview our library. For subscription information, please contact learning-admin@cisco.com.

FILTERS

More

DELIVERY TYPE

- □ Courses (1)
- □ Learning Collections (1)
- □ Video (1)
- □ Assessment (1)

TECHNOLOGY

- □ Mobility & Wireless (3)
- □ Networking (3)
- □ Cloud (2)
- □ Data Center (1)
- □ Security (1)

Clear All Filters

4 results found (0 filters applied | Clear All Filters

Sort Order: Relevance (Default)

Results per page: 10

FREE Demo

★★★★☆

Implementing and Configuring Cisco Identity Services Engine (SISE) v3.0

Courses
Security
CCNP, Security

40hr 0min

Not subscribed

★★★★☆

Cisco Prime Infrastructure Release 3.0

Learning Collections
Cisco UCS C-Series Rack-Mount Servers
Cloud, Data Center, Mobility & Wireless, Networking

3hr 19min

Not subscribed

★★★★☆

Cisco Prime Infrastructure Rel 3.0: How High Availability Works

Video
Cloud, Mobility & Wireless, Networking

0hr 8min

digital-learning.cisco.com

Содержание

1. **Политики сегментация как основа безопасности.**

2. **Много сценариев одного решения:**
   - Безопасный проводной доступ
   - Гостевой доступ к Wi-Fi сети
   - Администрирование устройств (TACACS+)
   - Личные устройства в корпоративной среде (BYOD)
   - Профилирование устройств (Profiling)
   - Проверка состояния устройств (Posture)

3. **Пошаговые рекомендации по разворачиванию:**
   - Лицензирование, и его особенности для ISE 3.0;
   - Типы узлов (Nodes), их назначение и количество;
   - Контролируемое и безопасное внедрение;

4. **Подготовка к внедрению:**
   - Что нужно знать, приступая к внедрению?
   - ISE Planning & Pre-Deployment Checklists
   - HLD (High Level Design)
   - ISE Size & Scale
   - How to troubleshoot ISE

Cisco Secure Zero Trust

#1

A comprehensive approach to securing all access across your people, applications, and environments.

Workforce

Ensure only the right users and secure devices can access applications.

Workplace

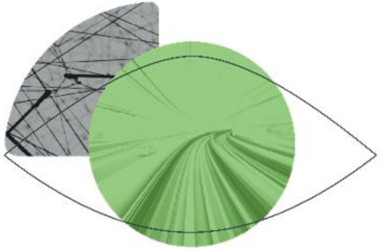
Secure all user and device connections across your network, including IoT.

Workloads

Secure all connections within your apps, across multi-cloud.

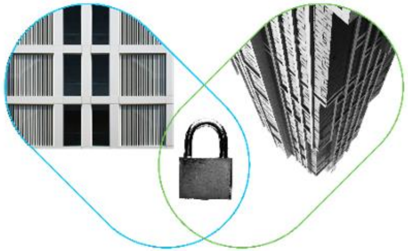
The Foundations of Zero Trust in Your Workplace

Visibility



Grant the right level of network access to users across domains

Segmentation



Shrink zones of trust and grant access based on least privilege

Containment

Automate containment of infected endpoints and revoke network access

ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Cisco ISE

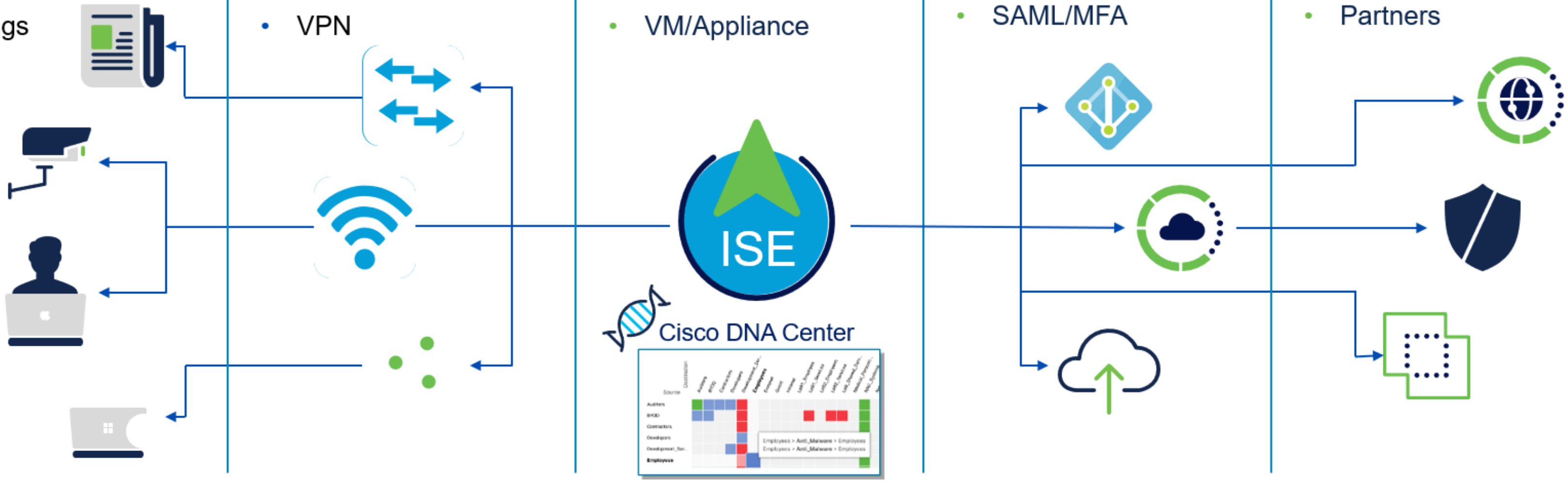
- Standalone ISE
- Multi-node ISE
- VM/Appliance

Identity Services

- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

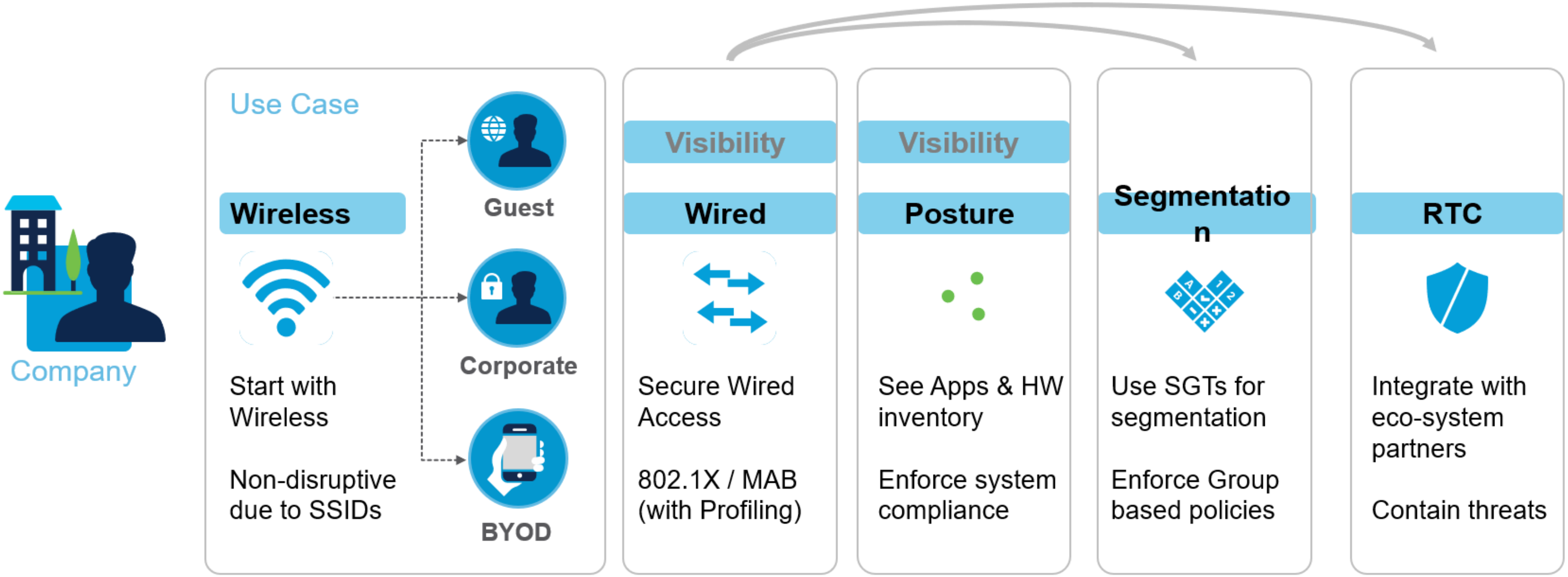
- Cloud Analytics
- Secure Firewall
- Partners



A Typical Journey

Not a standard or recommended approach

Each use case may be the end goal



Company

Use Case

Wireless

Guest

Corporate

BYOD

Start with Wireless

Non-disruptive due to SSIDs

Visibility

Wired

Secure Wired Access

802.1X / MAB (with Profiling)

Visibility

Posture

See Apps & HW inventory

Enforce system compliance

Segmentatio
n

Use SGTs for segmentation

Enforce Group based policies

RTC

Integrate with eco-system partners

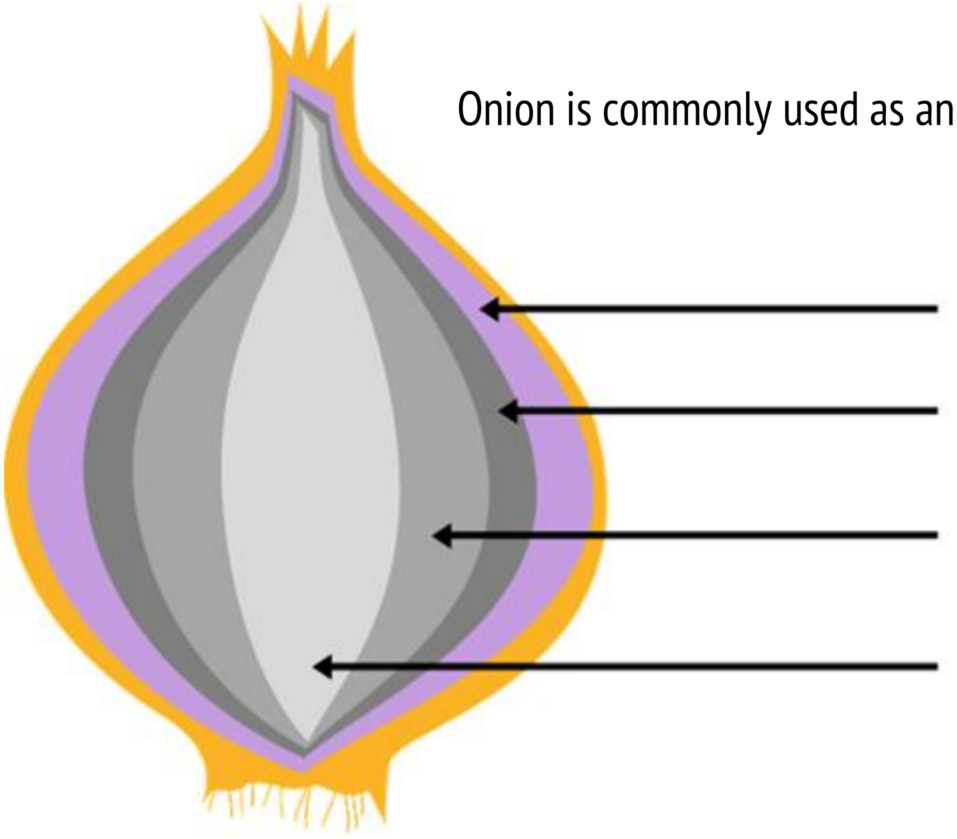
Contain threats

Defense-in-Depth Strategy #1

- Defense in depth can be considered a building block of other security design principles.
- Defense in depth is a philosophy that provides layered security to a system.
- The complexity of modern systems can make defense in depth implementation difficult.
- Defense in depth (if properly configured and monitored) minimizes the probability that the efforts of malicious hackers will succeed.
- Various components will be involved to implement the strategy of defense in depth successfully.

Defense-in-Depth Strategy (Cont.)

Onion is commonly used as an analogy of defense-in-depth strategy.



FIREWALL

Intrusion Prevention System

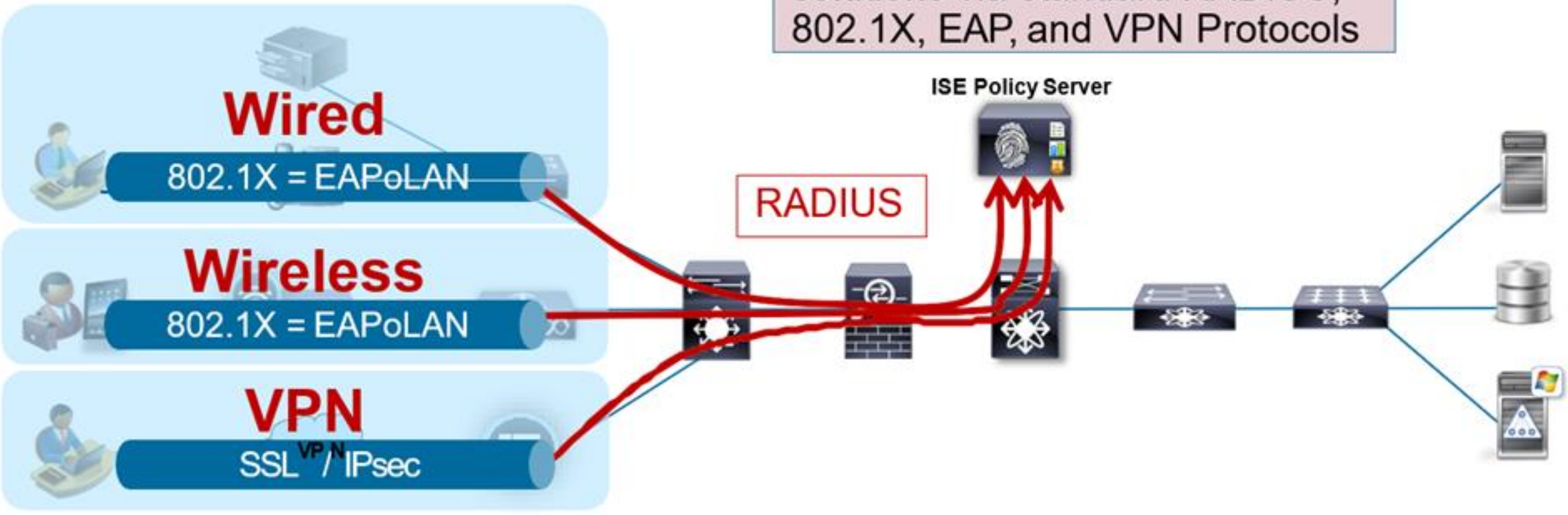
Authentication, Authorization, Accounting

Hardened Configuration

ISE is a Standards-Based AAA Server

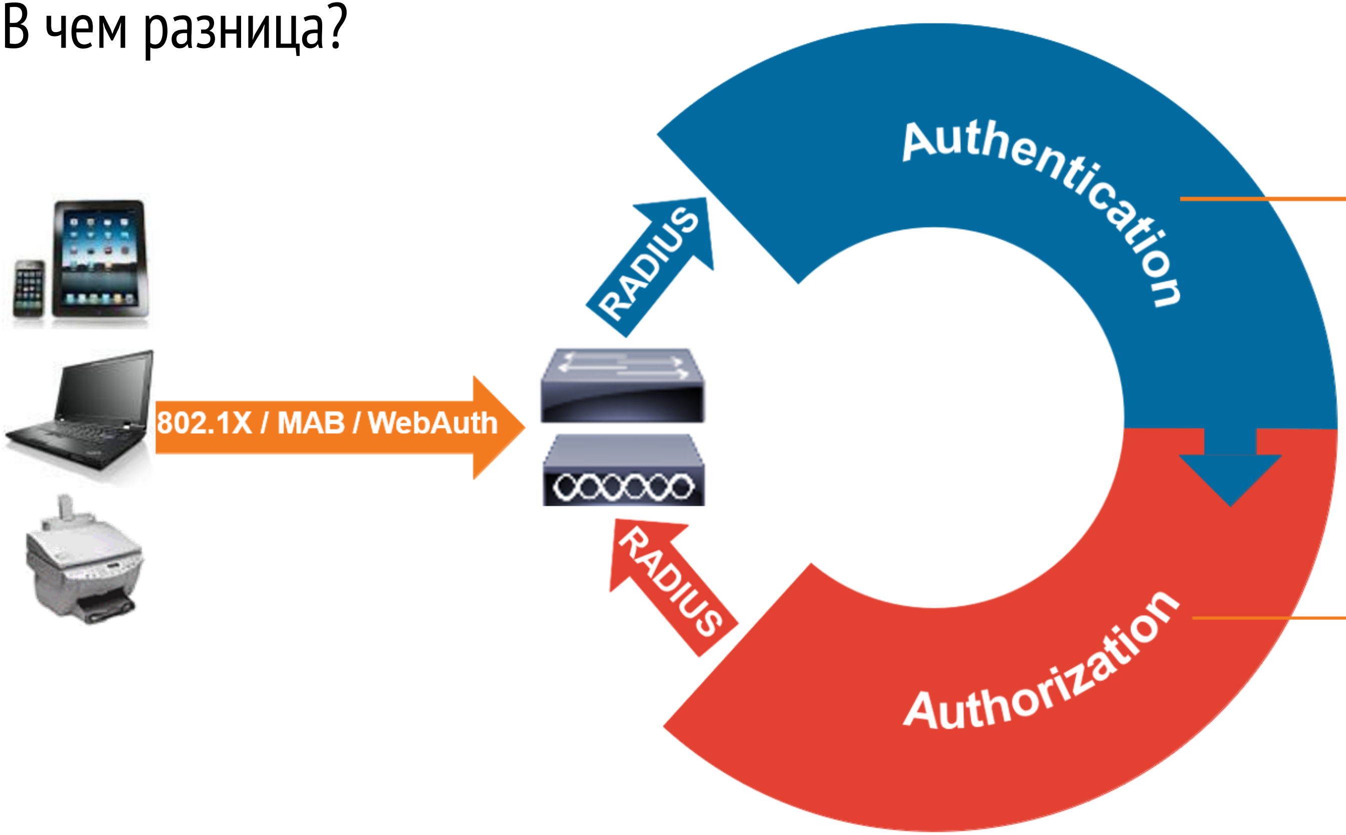
Должна быть реализована поддержка всевозможных методов подключения

Supports Cisco and 3rd-Party solutions via standard RADIUS, 802.1X, EAP, and VPN Protocols



Authentication and Authorization

В чем разница?

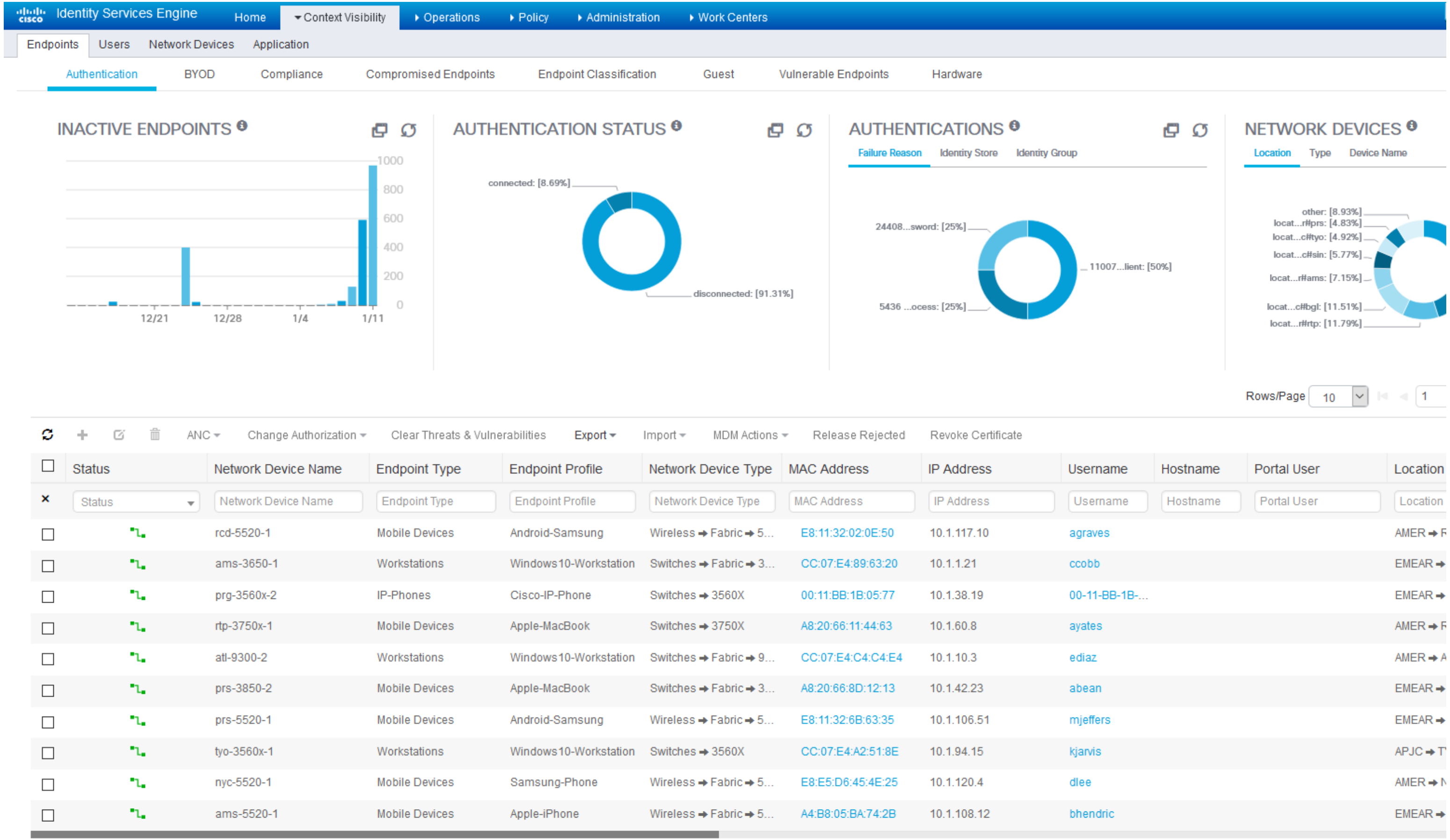


Who/what the endpoint is.

+ context

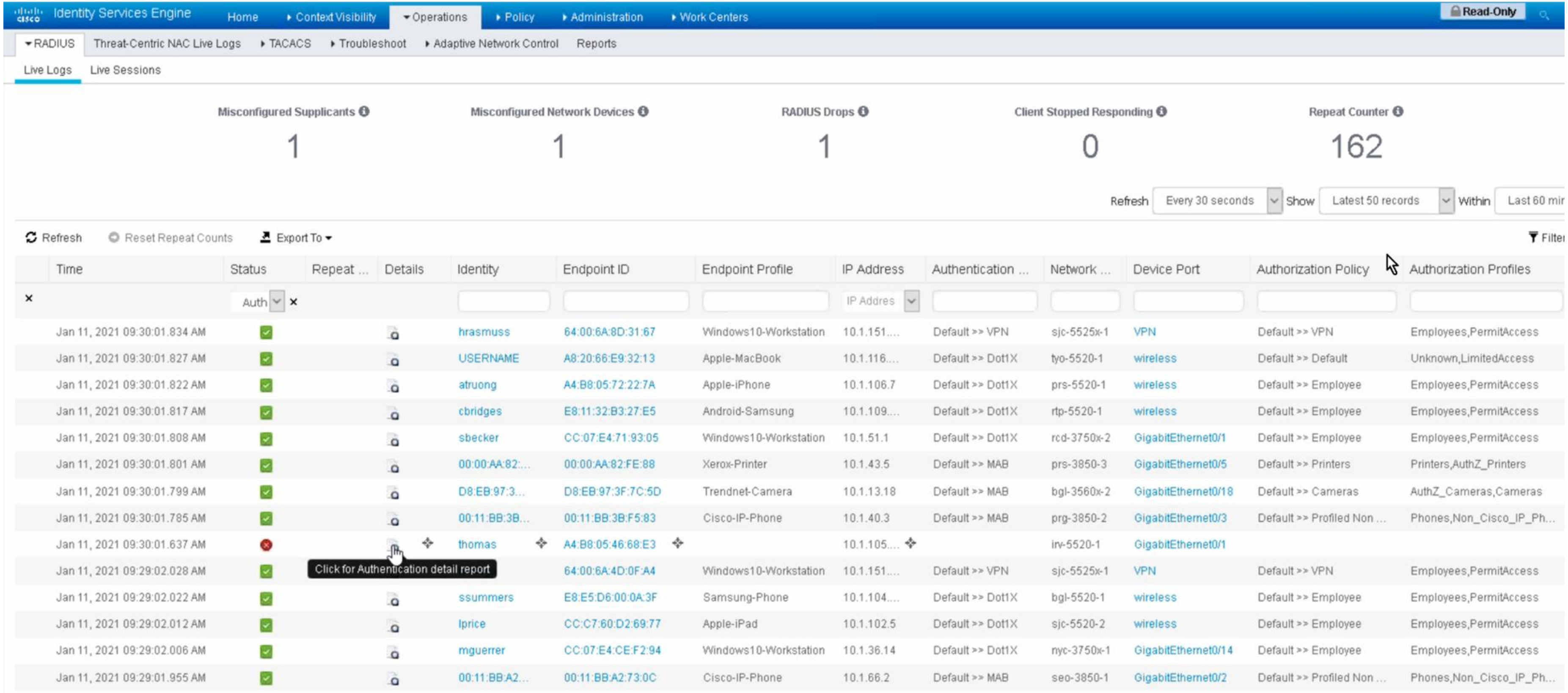
What the endpoint has access to.

What About That 3rd “A” in “AAA”?



□	Status	Network Device Name	Endpoint Type	Endpoint Profile	Network Device Type	MAC Address	IP Address	Username	Hostname	Portal User	Location
×	Status	Network Device Name	Endpoint Type	Endpoint Profile	Network Device Type	MAC Address	IP Address	Username	Hostname	Portal User	Location
□		rcd-5520-1	Mobile Devices	Android-Samsung	Wireless ➔ Fabric ➔ 5...	E8:11:32:02:0E:50	10.1.117.10	agraves			AMER ➔ F
□		ams-3650-1	Workstations	Windows10-Workstation	Switches ➔ Fabric ➔ 3...	CC:07:E4:89:63:20	10.1.1.21	ccobb			EMEAR ➔
□		prg-3560x-2	IP-Phones	Cisco-IP-Phone	Switches ➔ 3560X	00:11:BB:1B:05:77	10.1.38.19	00-11-BB-1B-...			EMEAR ➔
□		rtp-3750x-1	Mobile Devices	Apple-MacBook	Switches ➔ 3750X	A8:20:66:11:44:63	10.1.60.8	ayates			AMER ➔ F
□		atl-9300-2	Workstations	Windows10-Workstation	Switches ➔ Fabric ➔ 9...	CC:07:E4:C4:C4:E4	10.1.10.3	ediaz			AMER ➔ A
□		prs-3850-2	Mobile Devices	Apple-MacBook	Switches ➔ Fabric ➔ 3...	A8:20:66:8D:12:13	10.1.42.23	abean			EMEAR ➔
□		prs-5520-1	Mobile Devices	Android-Samsung	Wireless ➔ Fabric ➔ 5...	E8:11:32:6B:63:35	10.1.106.51	mjeffers			EMEAR ➔
□		tyo-3560x-1	Workstations	Windows10-Workstation	Switches ➔ 3560X	CC:07:E4:A2:51:8E	10.1.94.15	kjarvis			APJC ➔ T
□		nyc-5520-1	Mobile Devices	Samsung-Phone	Wireless ➔ Fabric ➔ 5...	E8:E5:D6:45:4E:25	10.1.120.4	dlee			AMER ➔ N
□		ams-5520-1	Mobile Devices	Apple-iPhone	Wireless ➔ Fabric ➔ 5...	A4:B8:05:BA:74:2B	10.1.108.12	bhendric			EMEAR ➔

Detailed Visibility into Passed/Failed Attempts

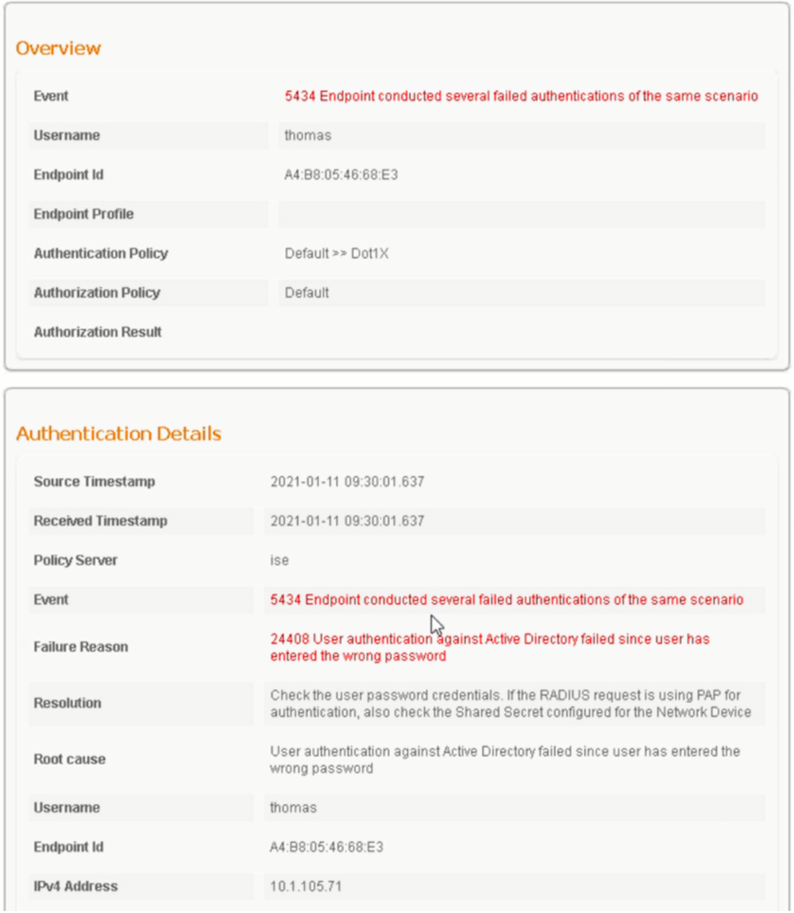


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
1	1	1	0	162

Refresh: Every 30 seconds · Show: Latest 50 records · Within: Last 60 mir

Time	Status	Repeat ...	Details	Identity	Endpoint ID	Endpoint Profile	IP Address	Authentication ...	Network ...	Device Port	Authorization Policy	Authorization Profiles
	Auth						IP Addres					
Jan 11, 2021 09:30:01.834 AM	✓			hrasmuss	64:00:6A:8D:31:67	Windows10-Workstation	10.1.151....	Default >> VPN	sjc-5525x-1	VPN	Default >> VPN	Employees,PermitAccess
Jan 11, 2021 09:30:01.827 AM	✓			USERNAME	A8:20:66:E9:32:13	Apple-MacBook	10.1.116....	Default >> Dot1X	tyo-5520-1	wireless	Default >> Default	Unknown,LimitedAccess
Jan 11, 2021 09:30:01.822 AM	✓			atruong	A4:B8:05:72:22:7A	Apple-iPhone	10.1.106.7	Default >> Dot1X	prs-5520-1	wireless	Default >> Employee	Employees,PermitAccess
Jan 11, 2021 09:30:01.817 AM	✓			cbridges	E8:11:32:B3:27:E5	Android-Samsung	10.1.109....	Default >> Dot1X	rtp-5520-1	wireless	Default >> Employee	Employees,PermitAccess
Jan 11, 2021 09:30:01.808 AM	✓			sbecker	CC:07:E4:71:93:05	Windows10-Workstation	10.1.51.1	Default >> Dot1X	rcd-3750x-2	GigabitEthernet0/1	Default >> Employee	Employees,PermitAccess
Jan 11, 2021 09:30:01.801 AM	✓			00:00:AA:82:...	00:00:AA:82:FE:88	Xerox-Printer	10.1.43.5	Default >> MAB	prs-3850-3	GigabitEthernet0/5	Default >> Printers	Printers,AuthZ_Printers
Jan 11, 2021 09:30:01.799 AM	✓			D8:EB:97:3...	D8:EB:97:3F:7C:5D	Trendnet-Camera	10.1.13.18	Default >> MAB	bgl-3560x-2	GigabitEthernet0/18	Default >> Cameras	AuthZ_Cameras,Cameras
Jan 11, 2021 09:30:01.785 AM	✓			00:11:BB:3B...	00:11:BB:3B:F5:83	Cisco-IP-Phone	10.1.40.3	Default >> MAB	prg-3850-2	GigabitEthernet0/3	Default >> Profiled Non ...	Phones,Non_Cisco_IP_Ph...
Jan 11, 2021 09:30:01.637 AM	✗			thomas	A4:B8:05:46:68:E3		10.1.105....		irv-5520-1	GigabitEthernet0/1		
Jan 11, 2021 09:29:02.028 AM	✓		Click for Authentication detail report		64:00:6A:4D:0F:A4	Windows10-Workstation	10.1.151....	Default >> VPN	sjc-5525x-1	VPN	Default >> VPN	Employees,PermitAccess
Jan 11, 2021 09:29:02.022 AM	✓			ssummers	E8:E5:D6:00:0A:3F	Samsung-Phone	10.1.104....	Default >> Dot1X	bgl-5520-1	wireless	Default >> Employee	Employees,PermitAccess
Jan 11, 2021 09:29:02.012 AM	✓			lprice	CC:C7:60:D2:69:77	Apple-iPad	10.1.102.5	Default >> Dot1X	sjc-5520-2	wireless	Default >> Employee	Employees,PermitAccess
Jan 11, 2021 09:29:02.006 AM	✓			mguerrer	CC:07:E4:CE:F2:94	Windows10-Workstation	10.1.36.14	Default >> Dot1X	nyc-3750x-1	GigabitEthernet0/14	Default >> Employee	Employees,PermitAccess
Jan 11, 2021 09:29:01.955 AM	✓			00:11:BB:A2...	00:11:BB:A2:73:0C	Cisco-IP-Phone	10.1.66.2	Default >> MAB	seo-3850-1	GigabitEthernet0/2	Default >> Profiled Non ...	Phones,Non_Cisco_IP_Ph...

Detailed Visibility into Passed/Failed Attempts

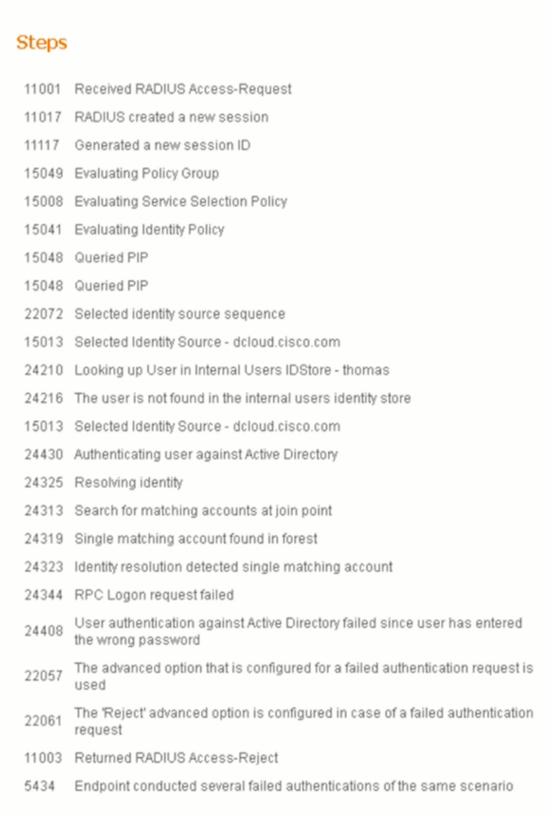


Overview

Event	5434 Endpoint conducted several failed authentications of the same scenario
Username	thomas
Endpoint Id	A4:B8:05:46:68:E3
Endpoint Profile	
Authentication Policy	Default >> Dot1X
Authorization Policy	Default
Authorization Result	

Authentication Details

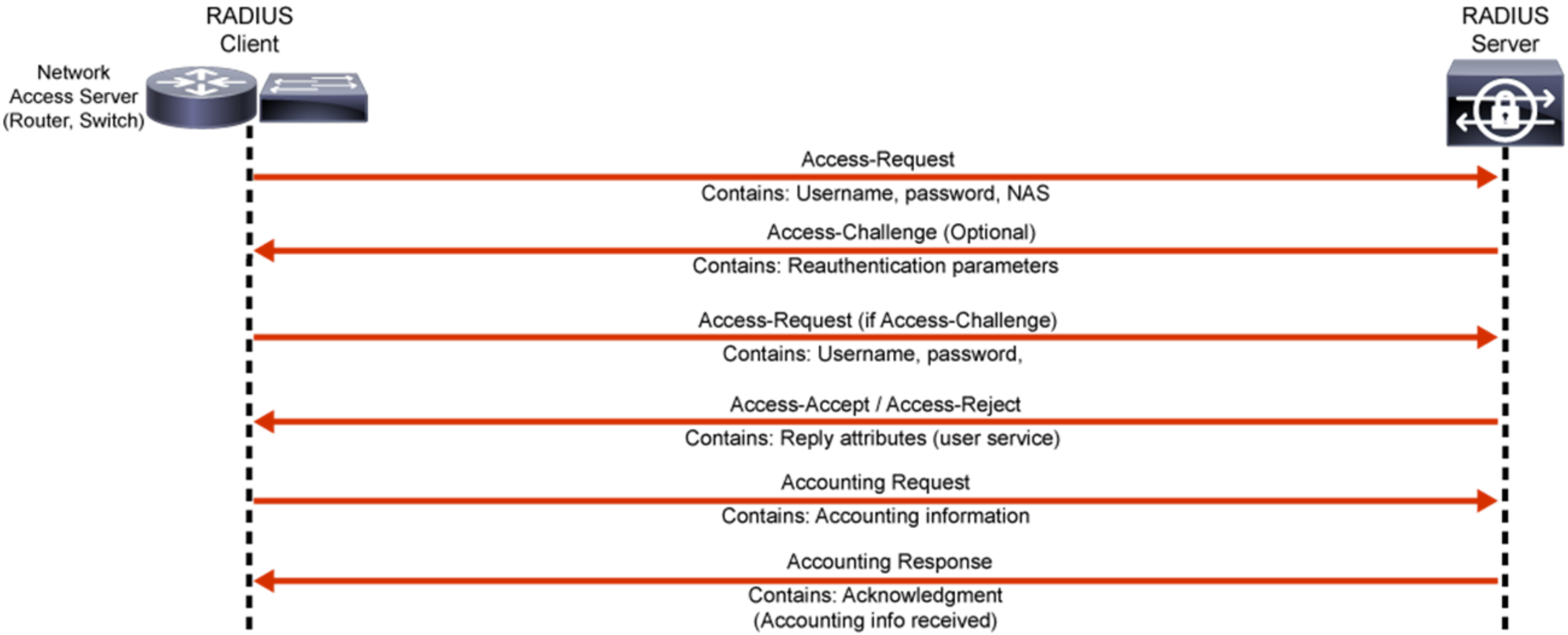
Source Timestamp	2021-01-11 09:30:01.637
Received Timestamp	2021-01-11 09:30:01.637
Policy Server	ise
Event	5434 Endpoint conducted several failed authentications of the same scenario
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Resolution	Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device
Root cause	User authentication against Active Directory failed since user has entered the wrong password
Username	thomas
Endpoint Id	A4:B8:05:46:68:E3
IPv4 Address	10.1.105.71



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP
15048	Queried PIP
22072	Selected identity source sequence
15013	Selected Identity Source - dcloud.cisco.com
24210	Looking up User in Internal Users IDStore - thomas
24216	The user is not found in the internal users identity store
15013	Selected Identity Source - dcloud.cisco.com
24430	Authenticating user against Active Directory
24325	Resolving identity
24313	Search for matching accounts at join point
24319	Single matching account found in forest
24323	Identity resolution detected single matching account
24344	RPC Logon request failed
24408	User authentication against Active Directory failed since user has entered the wrong password
22057	The advanced option that is configured for a failed authentication request is used
22061	The 'Reject' advanced option is configured in case of a failed authentication request
11003	Returned RADIUS Access-Reject
5434	Endpoint conducted several failed authentications of the same scenario

Radius AAA Communications



RADIUS Client

Network Access Server (Router, Switch)

RADIUS Server

Access-Request

Contains: Username, password, NAS

Access-Challenge (Optional)

Contains: Reauthentication parameters

Access-Request (if Access-Challenge)

Contains: Username, password,

Access-Accept / Access-Reject

Contains: Reply attributes (user service)

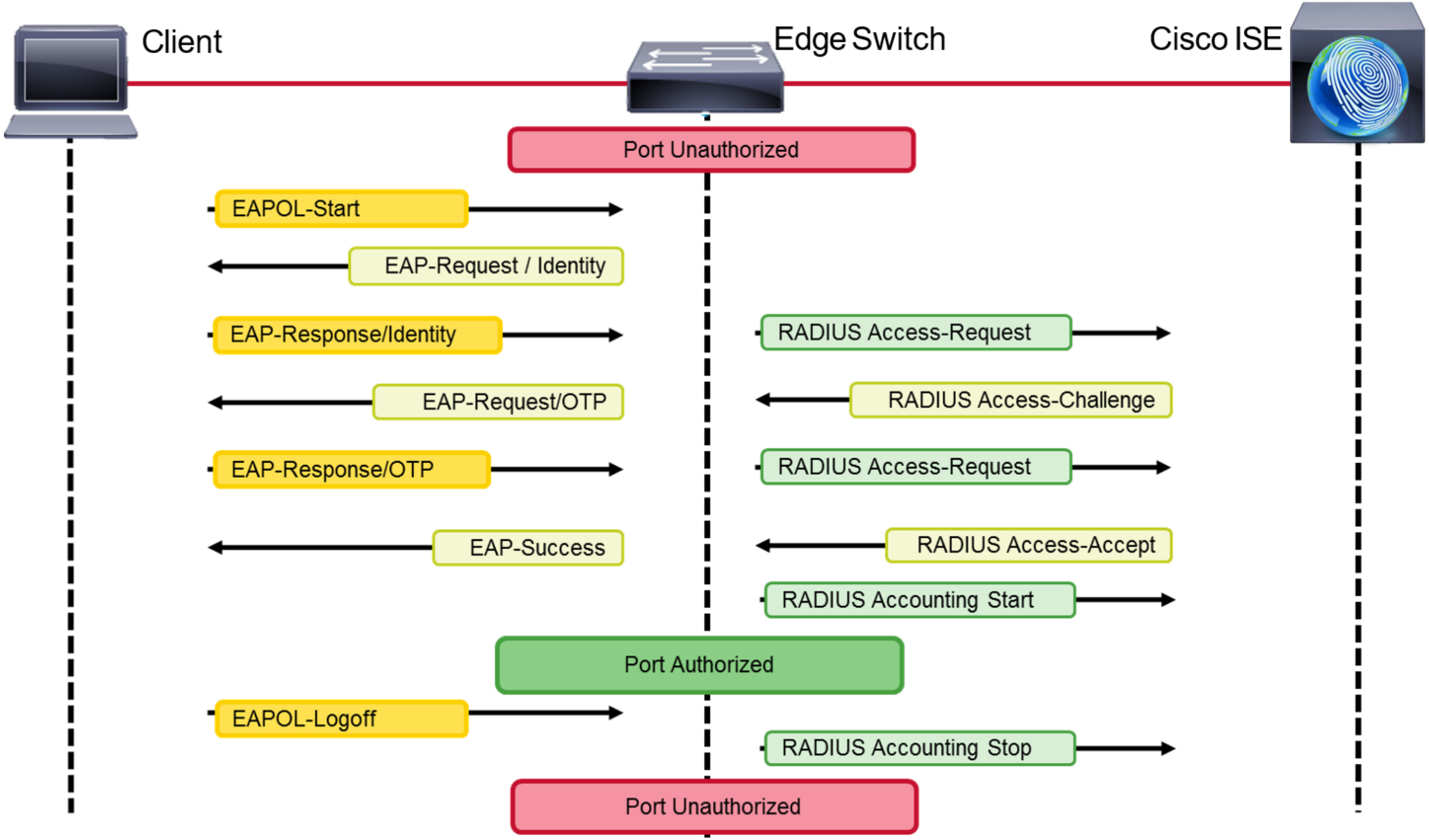
Accounting Request

Contains: Accounting information

Accounting Response

Contains: Acknowledgment
(Accounting info received)

802.1X Message Flow

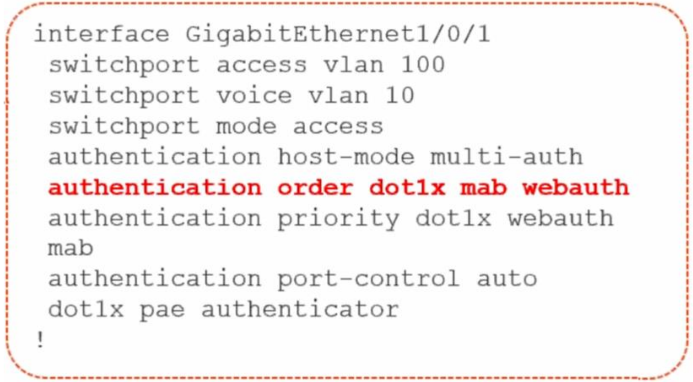


MAC Authentication Bypass (MAB)

Что это?

- Список MAC адресов устройств, которые могут «пропустить» authentication
- Это замена 802.1X?
  - Нет! Это исключение для устройств, которые не поддерживают Dot1x
- Список может быть локальным (например для порта коммутатора) или централизированным

Web Authentication



```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport voice vlan 10
 switchport mode access
 authentication host-mode multi-auth
 authentication order dot1x mab webauth
 authentication priority dot1x webauth
 mab
 authentication port-control auto
 dot1x pae authenticator
!
```

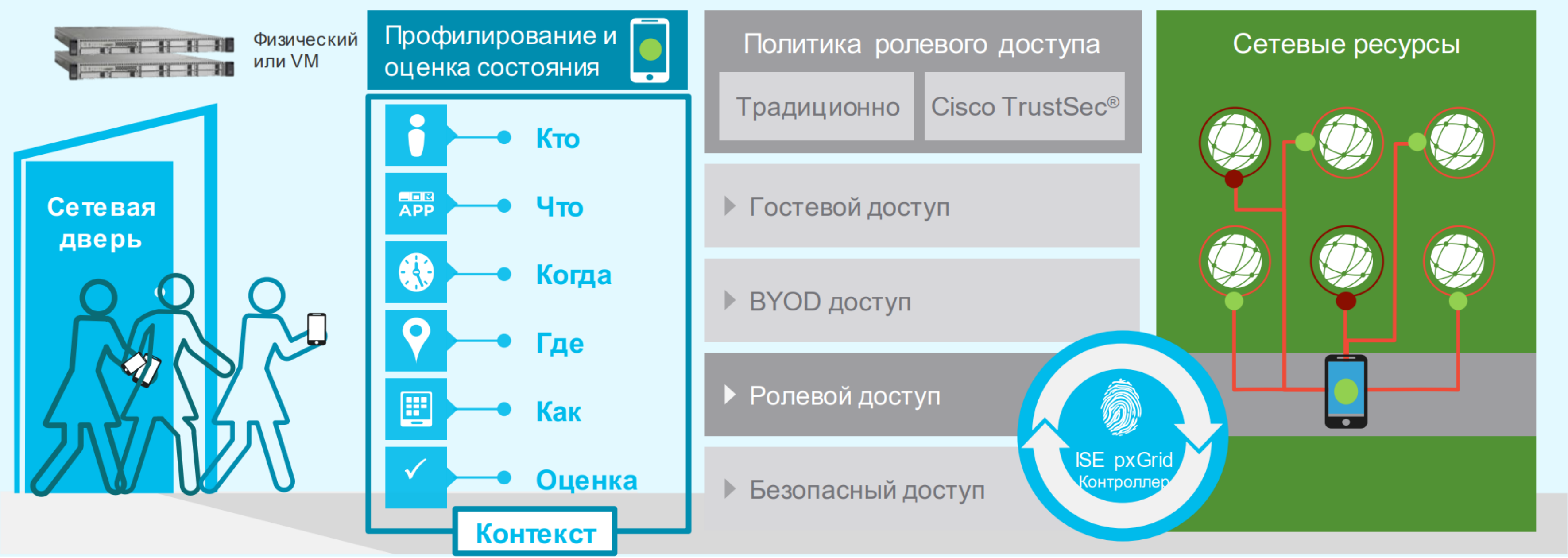
Что это?

- Authentication for Guest Users
- Authentication for Employees with Missing or Misconfigured Settings
- Это замена 802.1X?
  - Нет! Это исключение для устройств, которые не поддерживают Dot1x
- Настраивается локально либо централизованно

Cisco Identity Services Engine

#2

Централизованное решение для автоматизации контекстно-задаваемых политик доступа к сетевым ресурсам и обмена контекстом



Физический или VM

Сетевая дверь

Профилирование и оценка состояния

Кто

Что

Когда

Где

Как

Оценка

Контекст

Политика ролевого доступа

Традиционно

Cisco TrustSec®

Гостевой доступ

BYOD доступ

Ролевой доступ

Безопасный доступ

ISE pxGrid Контроллер

Сетевые ресурсы

Сценарии использования

Доступ к Wi-Fi сети
гостевой портал

Администрирование
логирование и доступ

Профилирование
устройств и пользователей

Безопасный доступ
использование ресурсов

BYOD
контроль личных устройств

Сдерживание угроз
распознавание и контроль

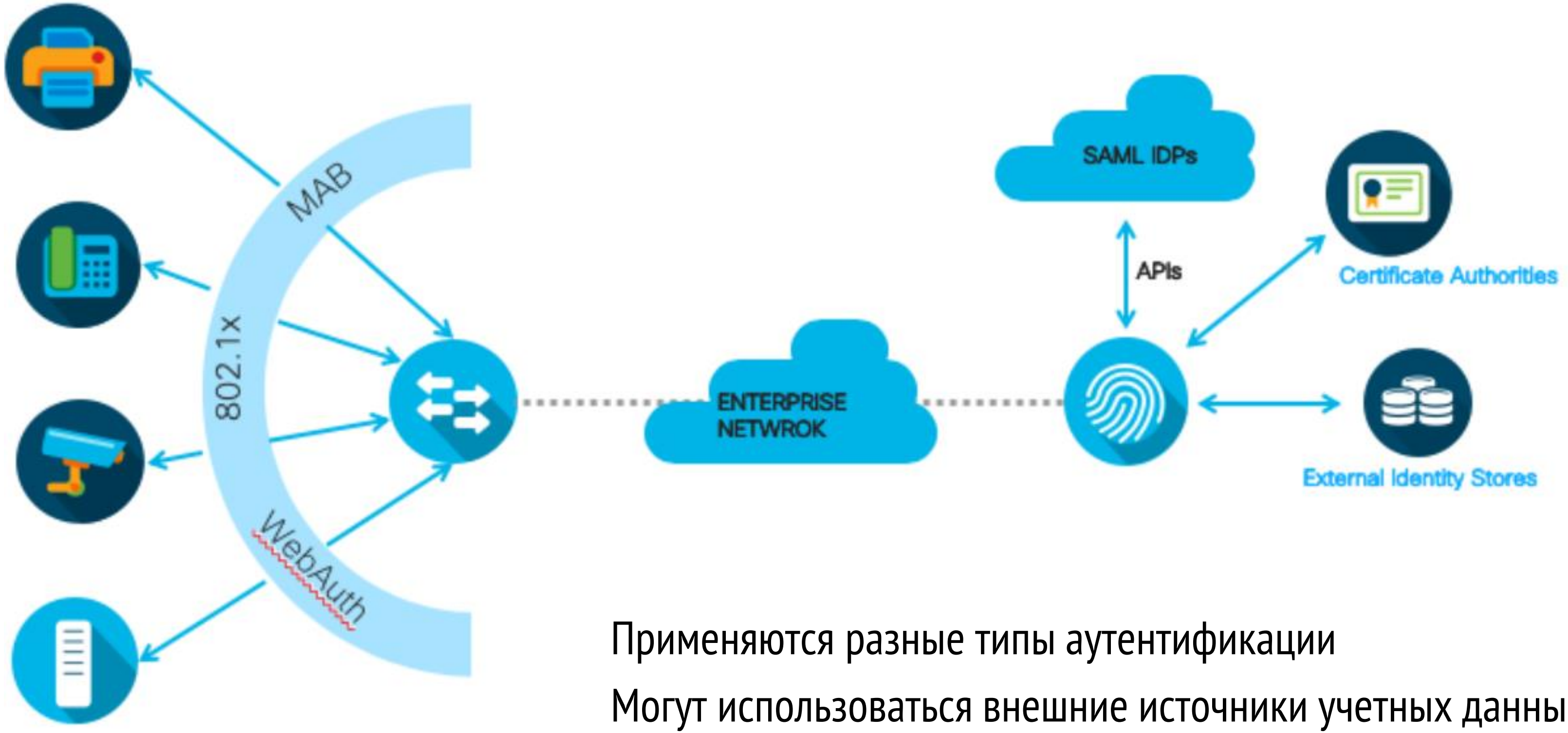
Сегментация

Контекст

Контроль
конечных устройств

Безопасный проводной доступ

Cisco ISE защищает от подключения неавторизованных пользователей и устройств



Применяются разные типы аутентификации

Могут использоваться внешние источники учетных данных

Безопасный проводной доступ

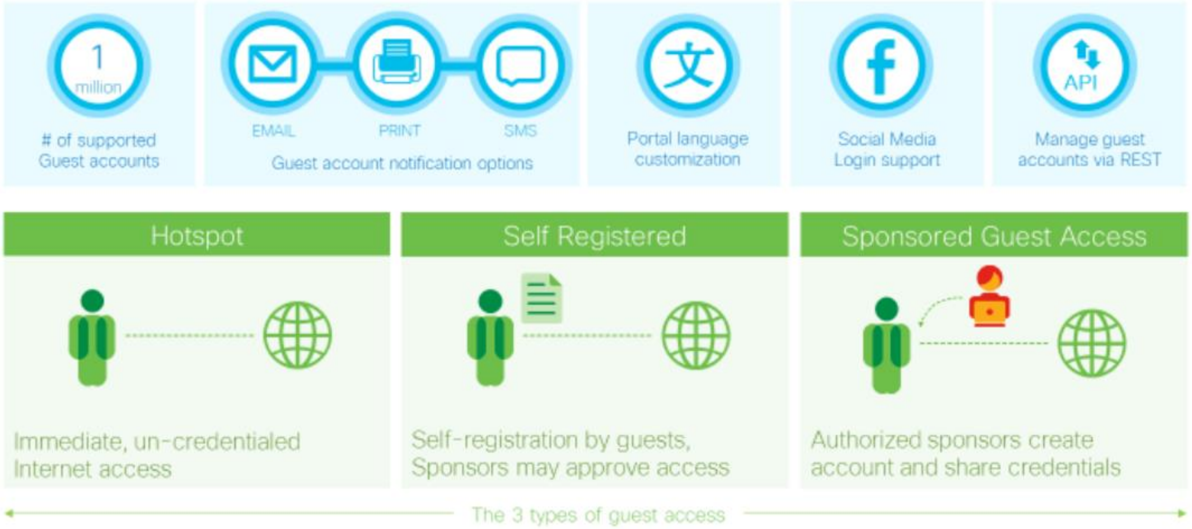
Как проверить результаты работы:

- В ISE перейти в раздел **Operations > RADIUS > Live Logs**
- В ISE перейти в раздел **Work Centers > Network Access > Reports** и выбрать «отчет»

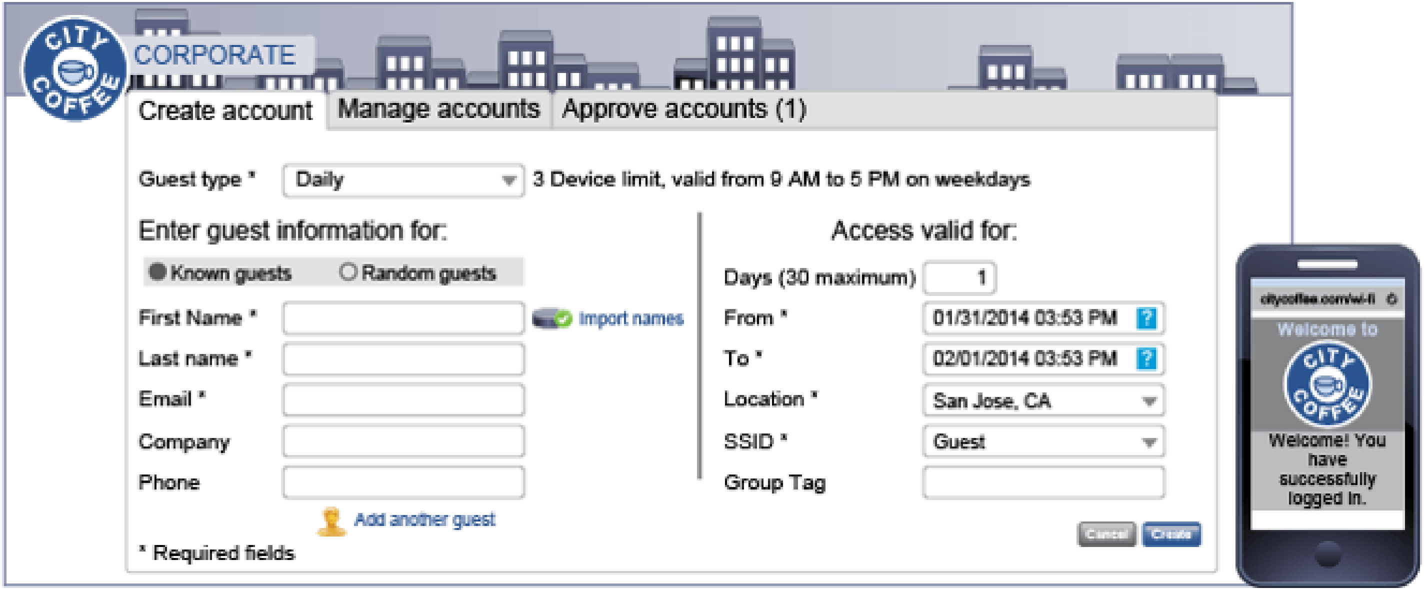
Дальше можно анализировать корректность и полноту настроенных политик.

Гостевой доступ пользователей к Wi-Fi сети

- **Hotspot** Guest Access
- Self-service or **Self-Registered** Guest Access
- **Sponsored** Guest Access (or Self-service Sponsor-Approved)


1 million
# of supported Guest accounts
EMAIL
PRINT
SMS
Guest account notification options
Portal language customization
Social Media Login support
API
Manage guest accounts via REST
Hotspot
Self Registered
Sponsored Guest Access
Immediate, un-credentialed Internet access
Self-registration by guests, Sponsors may approve access
Authorized sponsors create account and share credentials
The 3 types of guest access

Sponsored Guest Access



Create account | Manage accounts | Approve accounts (1)

Guest type * Daily ▾ 3 Device limit, valid from 9 AM to 5 PM on weekdays

Enter guest information for:

● Known guests ○ Random guests

First Name *	
Last name *	
Email *	
Company	
Phone	

* Required fields

Access valid for:

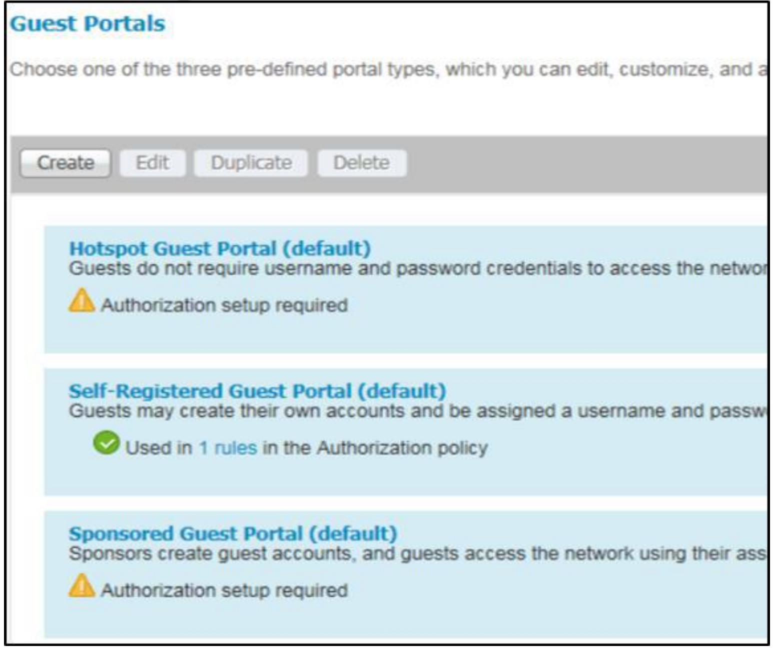
Days (30 maximum)	1
From *	01/31/2014 03:53 PM
To *	02/01/2014 03:53 PM
Location *	San Jose, CA
SSID *	Guest
Group Tag	

citycoffee.com/wi-fi

Welcome to

Welcome! You have successfully logged In.

Multiple Guest Portals



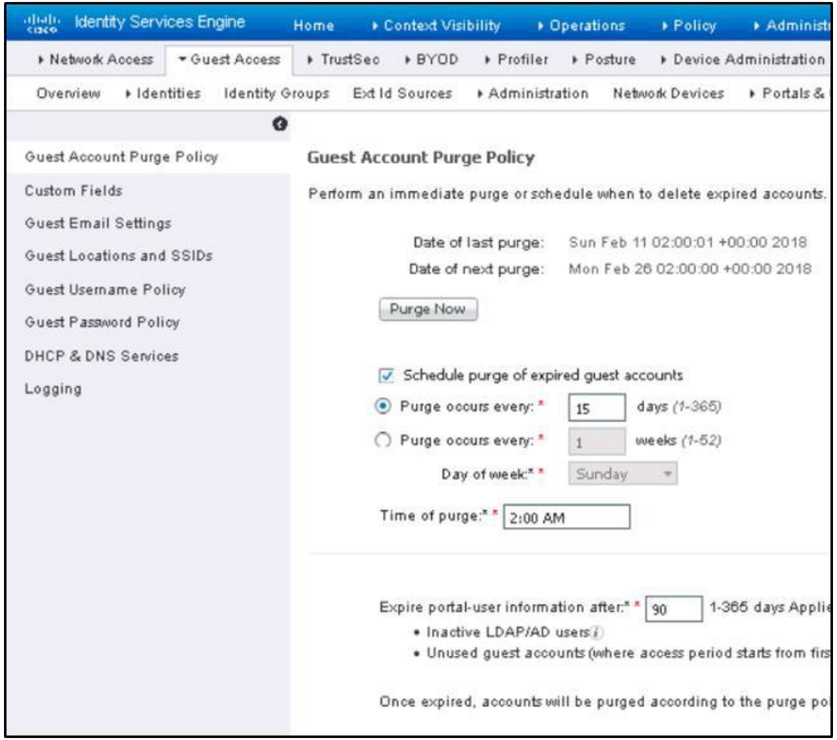
Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and a

Hotspot Guest Portal (default)
Guests do not require username and password credentials to access the networ
⚠ Authorization setup required

Self-Registered Guest Portal (default)
Guests may create their own accounts and be assigned a username and passw
✓ Used in 1 rules in the Authorization policy

Sponsored Guest Portal (default)
Sponsors create guest accounts, and guests access the network using their ass
⚠ Authorization setup required



Guest Account Purge Policy

Perform an immediate purge or schedule when to delete expired accounts.

Date of last purge: Sun Feb 11 02:00:01 +00:00 2018
Date of next purge: Mon Feb 26 02:00:00 +00:00 2018

☑ Schedule purge of expired guest accounts
● Purge occurs every: * 15 days (1-365)
○ Purge occurs every: * 1 weeks (1-52)
Day of week:* * Sunday
Time of purge:* * 2:00 AM

Expire portal-user information after:* * 90 1-365 days Applie
- Inactive LDAP/AD users
- Unused guest accounts (where access period starts from firs

Once expired, accounts will be purged according to the purge po

- Использование установленных политик безопасности и их «сроки жизни»;
- У нас нет в сети «неустановленных» пользователей, в случае расследования инциндентов ИБ
- Мы можем получать о пользователе другую информацию (User-agent, device name and so on).

Гостевой доступ пользователей к Wi-Fi сети

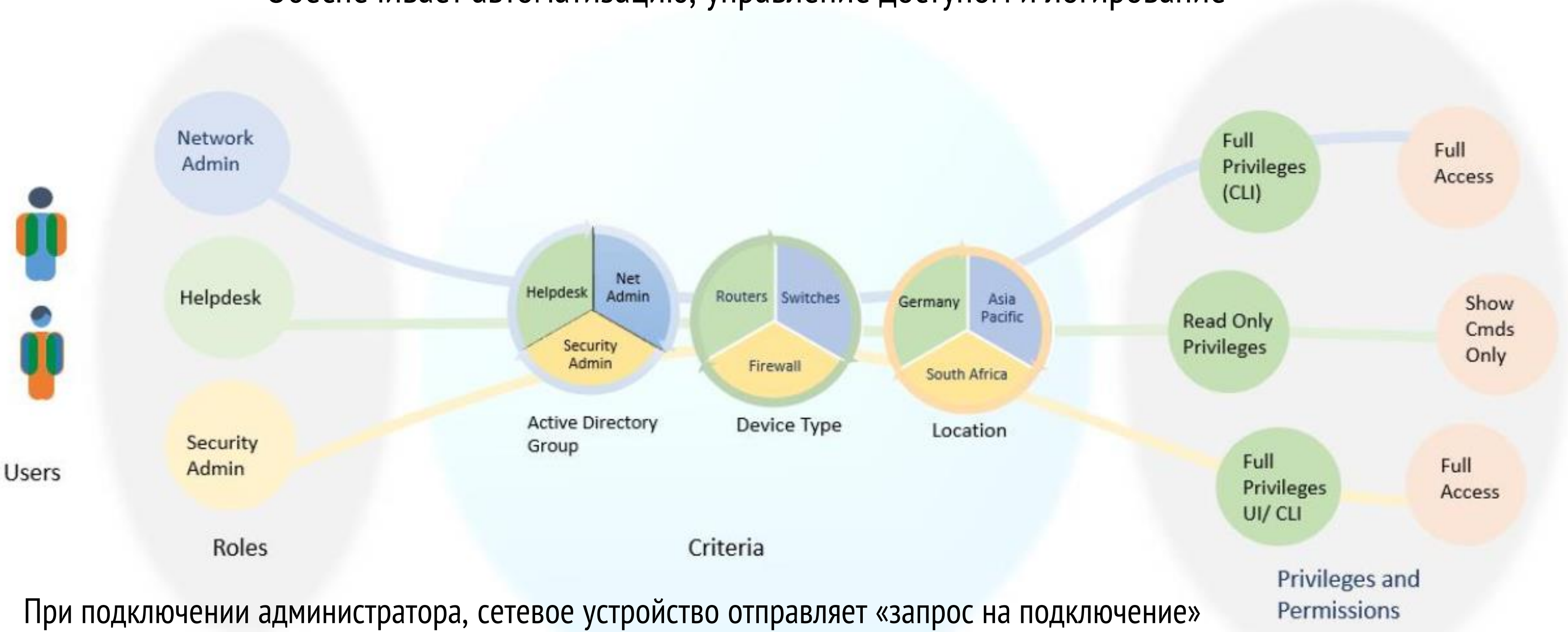
Как проверить результаты работы:

- В ISE перейти в раздел **Operations > RADIUS > Live Logs**
- В ISE перейти в раздел **Work Centers > Guest Access > Reports** и выбрать «отчет»

Дальше можно анализировать корректность и полноту настроенных политик.

Администрирование устройств (TACACS+)

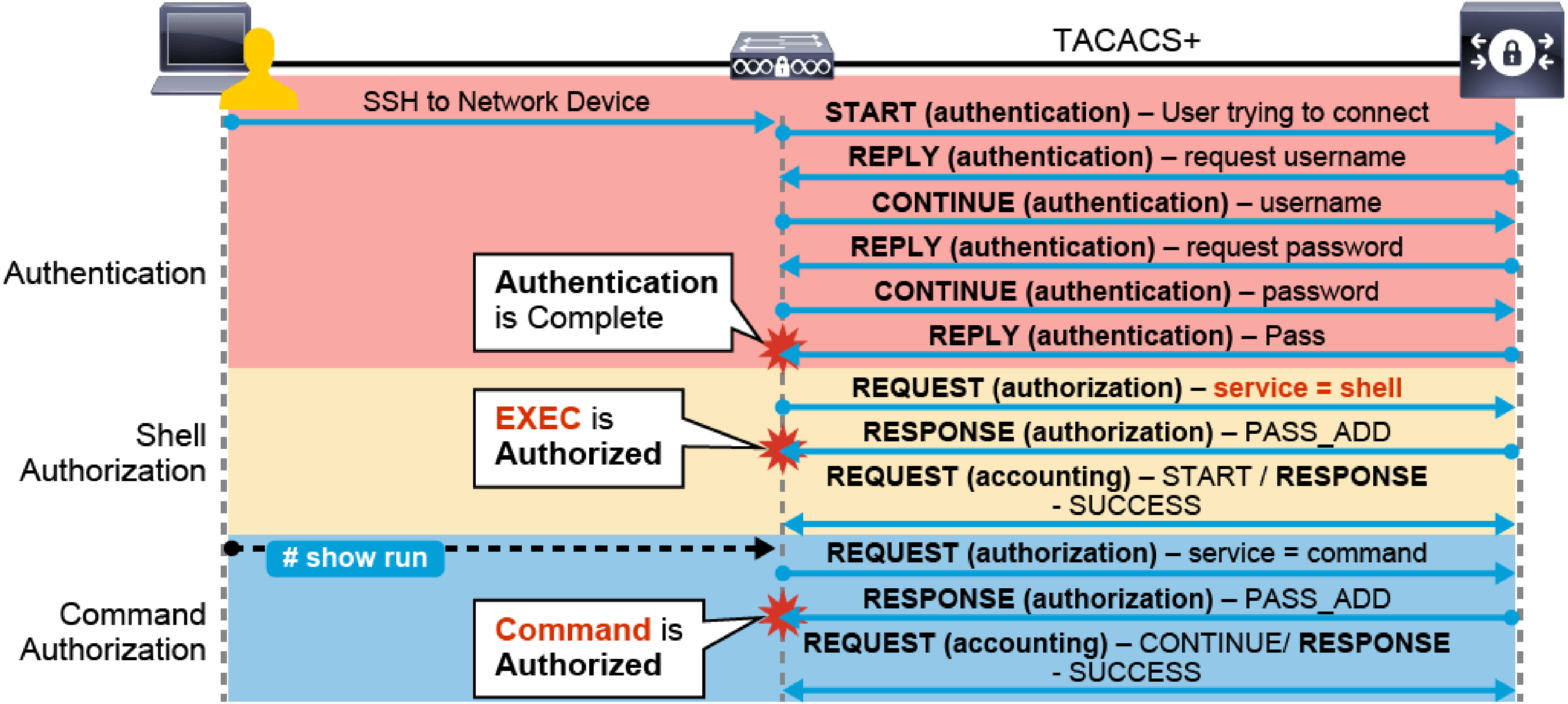
Обеспечивает автоматизацию, управление доступом и логирование



При подключении администратора, сетевое устройство отправляет «запрос на подключение»

ISE проводит сверку учетных данных и предоставляет доступ с установленным уровнем привилегий

Authentication Once + Authorization Many


TACACS+
SSH to Network Device
START (authentication) – User trying to connect
REPLY (authentication) – request username
CONTINUE (authentication) – username
REPLY (authentication) – request password
CONTINUE (authentication) – password
REPLY (authentication) – Pass
Authentication
Authentication is Complete
REQUEST (authorization) – service = shell
RESPONSE (authorization) – PASS_ADD
REQUEST (accounting) – START / RESPONSE - SUCCESS
Shell Authorization
EXEC is Authorized
# show run
REQUEST (authorization) – service = command
RESPONSE (authorization) – PASS_ADD
REQUEST (accounting) – CONTINUE/ RESPONSE - SUCCESS
Command Authorization
Command is Authorized

Администрирование устройств (TACACS+)

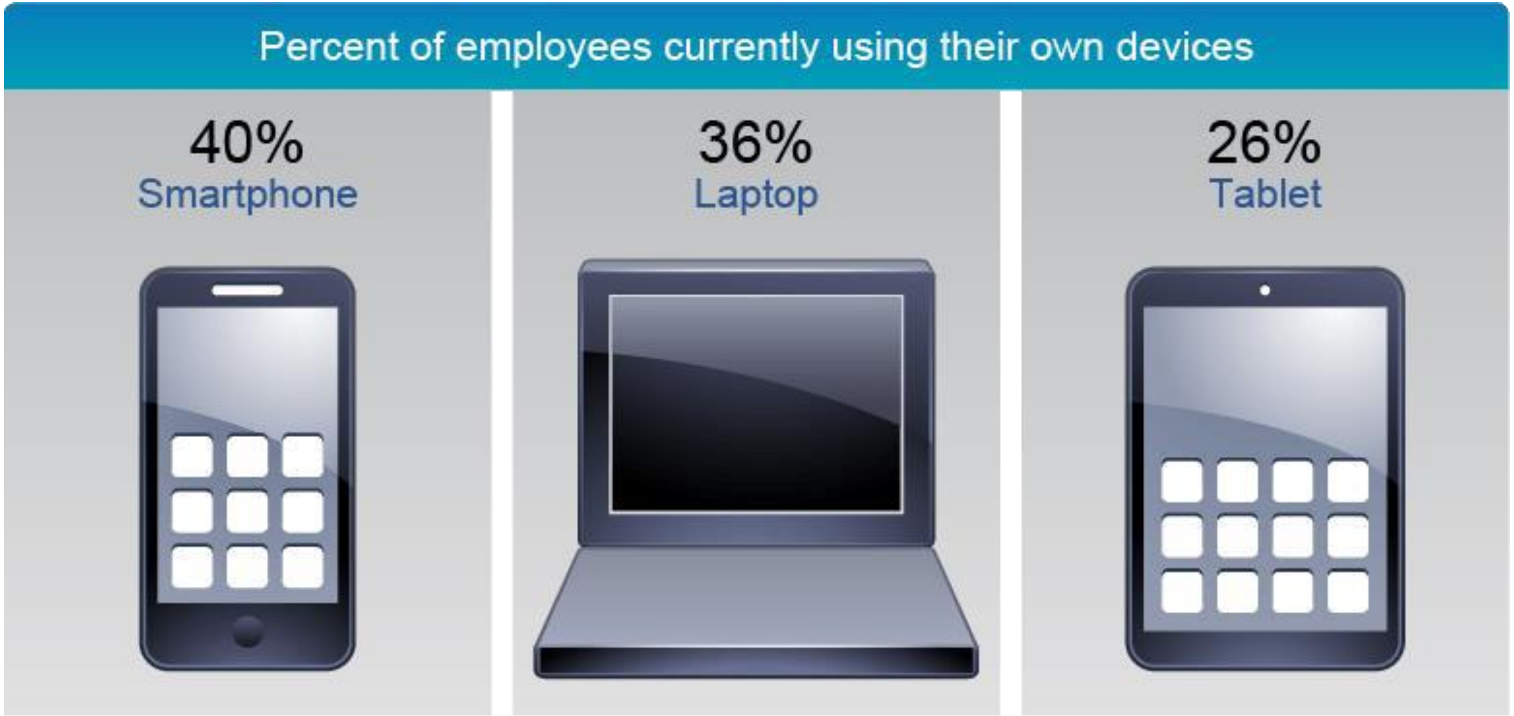
Как проверить результаты работы:

- В ISE перейти в раздел **Operations > TACACS > Live Logs**
- В ISE перейти в раздел **Work Centers > Device Administration > Reports** и выбрать «отчет»

Дальше можно анализировать корректность и полноту настроенных политик.

Личные устройства в корпоративной среде (BYOD)

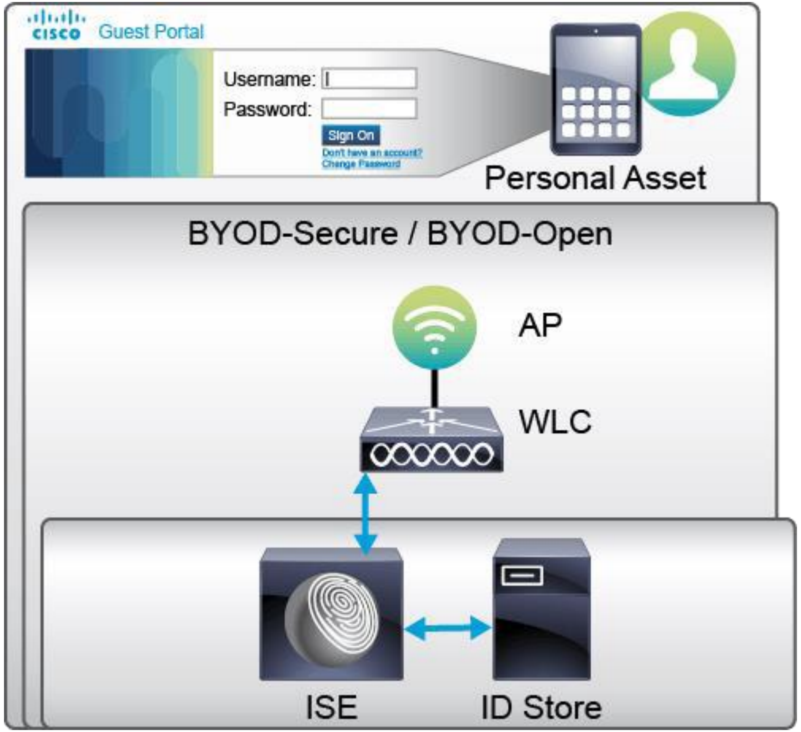
Use of personal devices can increase productivity.
Percentage of hand-held devices is growing.



Личные устройства в корпоративной среде (BYOD)

Алгоритм подключения персонального устройства

- User connects to Open SSID
- Redirected to WebAuth portal
- User enters employee or guest credentials
- Guest signs AUP and getsGuest access
- Employee redirected to BYOD provisioning portal
- Employee registers device
  - – Certificate Provisioning
  - – Downloads supplicant configuration
- Employee reconnects to the Secure SSID using EAP-TLS



Встроенный центр сертификации

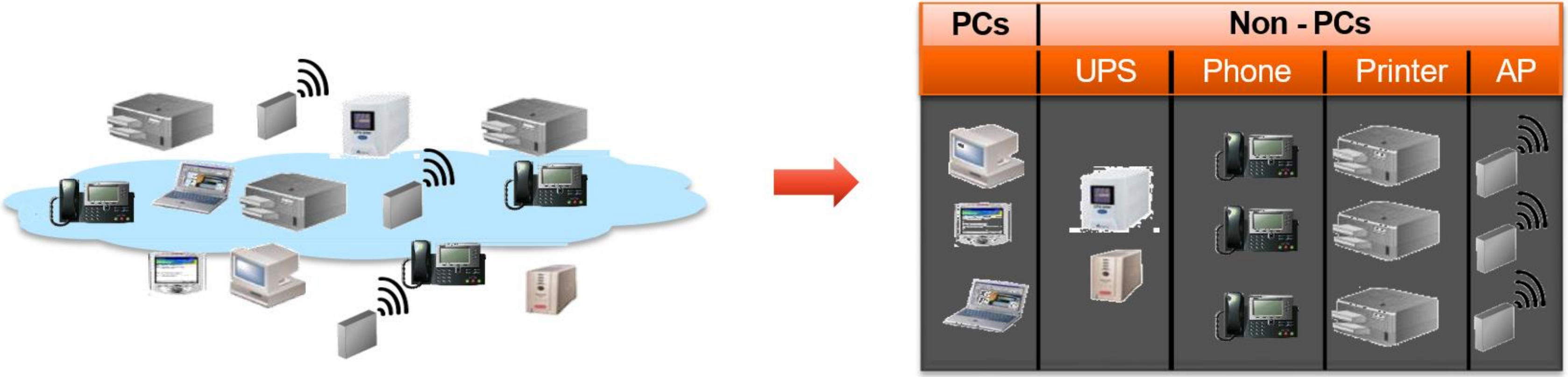
Портал для управления своими устройствами BYOD

Профилирование устройств (Profiling)

- **What ISE Profiling is:**

  Dynamic classification of every device that connects to network using the infrastructure.

  Provides the context of “What” is connected independent of user identity for use in accesspolicy decisions

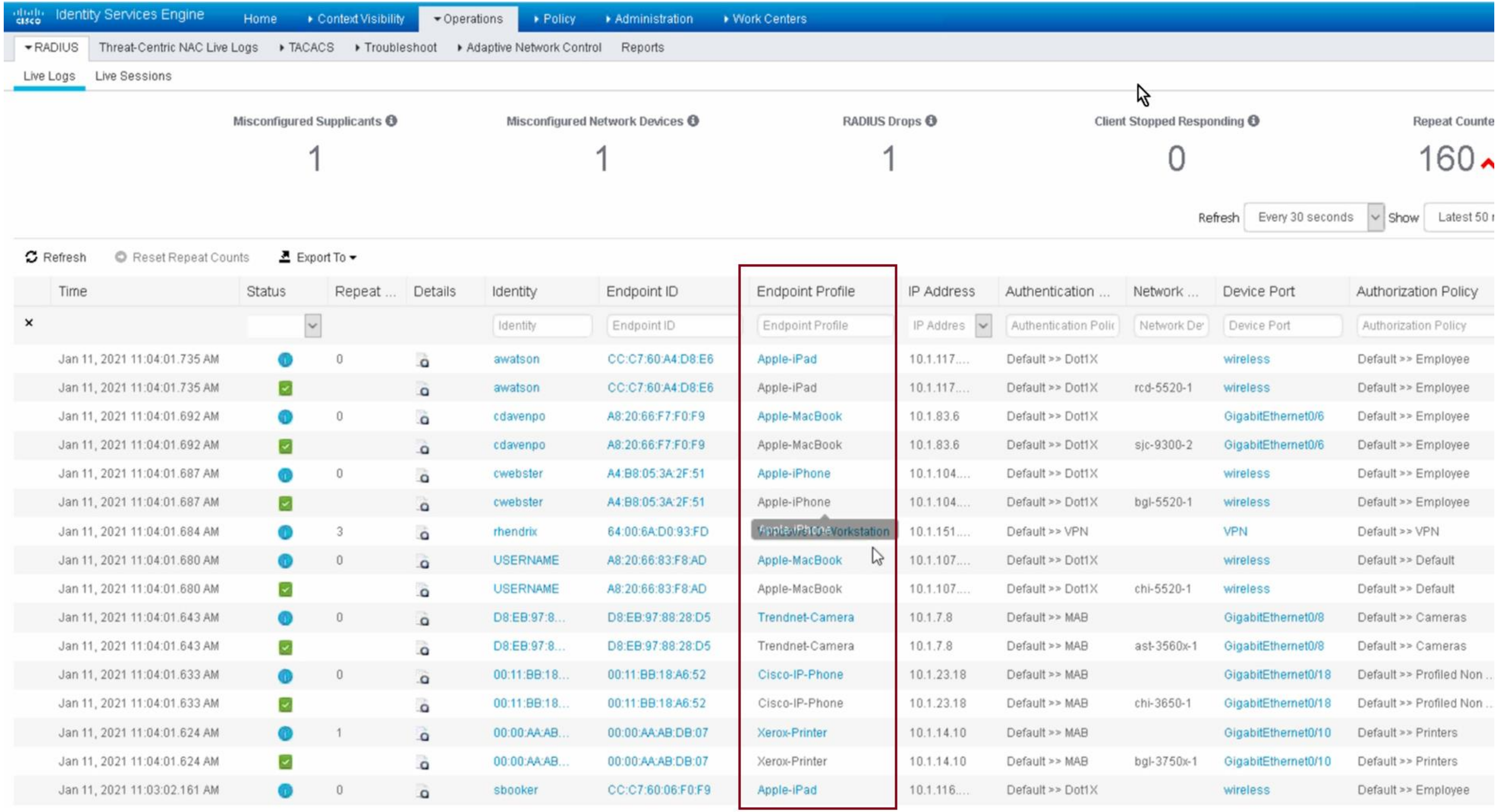


- **What Profiling is NOT:**

  An authentication mechanism.

  An exact science for device classification.

Profiling -> Live Logs



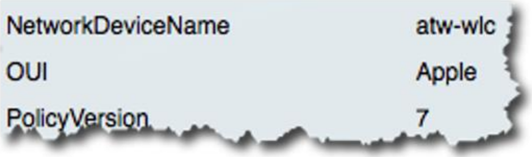
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counte
1	1	1	0	160

Refresh: Every 30 seconds | Show: Latest 50 r

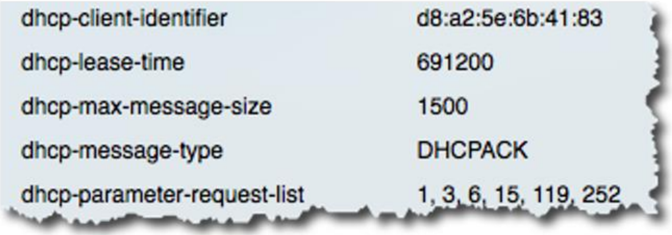
	Time	Status	Repeat ...	Details	Identity	Endpoint ID	Endpoint Profile	IP Address	Authentication ...	Network ...	Device Port	Authorization Policy
×					Identity	Endpoint ID	Endpoint Profile	IP Addres	Authentication Polic	Network De	Device Port	Authorization Policy
	Jan 11, 2021 11:04:01.735 AM	●	0	🔍	awatson	CC:C7:60:A4:D8:E6	Apple-iPad	10.1.117....	Default >> Dot1X		wireless	Default >> Employee
	Jan 11, 2021 11:04:01.735 AM	✓		🔍	awatson	CC:C7:60:A4:D8:E6	Apple-iPad	10.1.117....	Default >> Dot1X	rcd-5520-1	wireless	Default >> Employee
	Jan 11, 2021 11:04:01.692 AM	●	0	🔍	cdavenpo	A8:20:66:F7:F0:F9	Apple-MacBook	10.1.83.6	Default >> Dot1X		GigabitEthernet0/6	Default >> Employee
	Jan 11, 2021 11:04:01.692 AM	✓		🔍	cdavenpo	A8:20:66:F7:F0:F9	Apple-MacBook	10.1.83.6	Default >> Dot1X	sjc-9300-2	GigabitEthernet0/6	Default >> Employee
	Jan 11, 2021 11:04:01.687 AM	●	0	🔍	cwebster	A4:B8:05:3A:2F:51	Apple-iPhone	10.1.104....	Default >> Dot1X		wireless	Default >> Employee
	Jan 11, 2021 11:04:01.687 AM	✓		🔍	cwebster	A4:B8:05:3A:2F:51	Apple-iPhone	10.1.104....	Default >> Dot1X	bgl-5520-1	wireless	Default >> Employee
	Jan 11, 2021 11:04:01.684 AM	●	3	🔍	rhendrix	64:00:6A:D0:93:FD	Windows10-Workstation	10.1.151....	Default >> VPN		VPN	Default >> VPN
	Jan 11, 2021 11:04:01.680 AM	●	0	🔍	USERNAME	A8:20:66:83:F8:AD	Apple-MacBook	10.1.107....	Default >> Dot1X		wireless	Default >> Default
	Jan 11, 2021 11:04:01.680 AM	✓		🔍	USERNAME	A8:20:66:83:F8:AD	Apple-MacBook	10.1.107....	Default >> Dot1X	chi-5520-1	wireless	Default >> Default
	Jan 11, 2021 11:04:01.643 AM	●	0	🔍	D8:EB:97:8...	D8:EB:97:88:28:D5	Trendnet-Camera	10.1.7.8	Default >> MAB		GigabitEthernet0/8	Default >> Cameras
	Jan 11, 2021 11:04:01.643 AM	✓		🔍	D8:EB:97:8...	D8:EB:97:88:28:D5	Trendnet-Camera	10.1.7.8	Default >> MAB	ast-3560x-1	GigabitEthernet0/8	Default >> Cameras
	Jan 11, 2021 11:04:01.633 AM	●	0	🔍	00:11:BB:18...	00:11:BB:18:A6:52	Cisco-IP-Phone	10.1.23.18	Default >> MAB		GigabitEthernet0/18	Default >> Profiled Non ...
	Jan 11, 2021 11:04:01.633 AM	✓		🔍	00:11:BB:18...	00:11:BB:18:A6:52	Cisco-IP-Phone	10.1.23.18	Default >> MAB	chi-3650-1	GigabitEthernet0/18	Default >> Profiled Non ...
	Jan 11, 2021 11:04:01.624 AM	●	1	🔍	00:00:AA:AB...	00:00:AA:AB:DB:07	Xerox-Printer	10.1.14.10	Default >> MAB		GigabitEthernet0/10	Default >> Printers
	Jan 11, 2021 11:04:01.624 AM	✓		🔍	00:00:AA:AB...	00:00:AA:AB:DB:07	Xerox-Printer	10.1.14.10	Default >> MAB	bgl-3750x-1	GigabitEthernet0/10	Default >> Printers
	Jan 11, 2021 11:03:02.161 AM	●	0	🔍	sbooker	CC:C7:60:06:F0:F9	Apple-iPad	10.1.116....	Default >> Dot1X		wireless	Default >> Employee

Profiling Technology
How Do We Classify a Device?

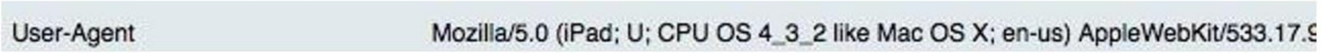
- Profiling uses signatures (similar to IPS)



NetworkDeviceName	atw-wlc
OUI	Apple
PolicyVersion	7



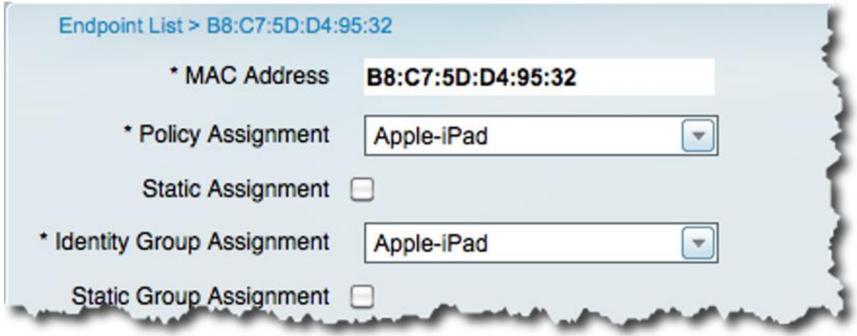
dhcp-client-identifier	d8:a2:5e:6b:41:83
dhcp-lease-time	691200
dhcp-max-message-size	1500
dhcp-message-type	DHCPACK
dhcp-parameter-request-list	1, 3, 6, 15, 119, 252



User-Agent	Mozilla/5.0 (iPad; U; CPU OS 4_3_2 like Mac OS X; en-us) AppleWebKit/533.17.9

- Probes are used to collect endpoint data

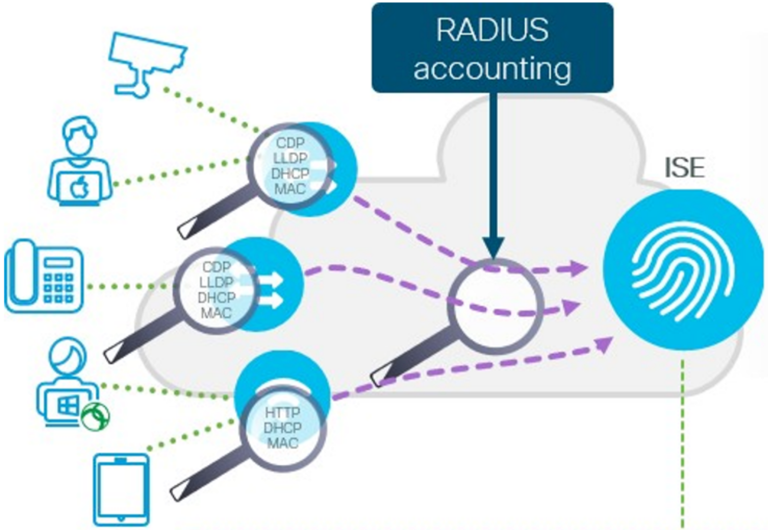
DHCP
HTTP
SNMP Query
RADIUS
SNMP Trap
DHCPSPAN
DNS
NMAP
NetFlow



Endpoint List > B8:C7:5D:D4:95:32

* MAC Address	B8:C7:5D:D4:95:32
* Policy Assignment	Apple-iPad
Static Assignment	□
* Identity Group Assignment	Apple-iPad
Static Group Assignment	□

Simplify Profiling with Device Sensor



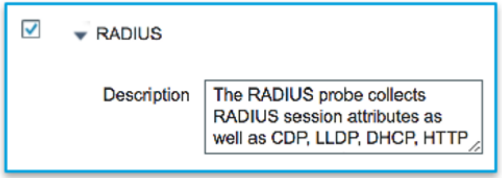
- MAC OUI
- CDP/LLDP
- DHCP
- HTTP (WLC only)
- mDNS,
- H323,
- MSI-Proxy (4k only)

Data From Device Sensor + Profile Conditions = PROFILED

Example:
MAC OUI + Lexmark

If DHCP Class ID
Contains E260dn

It's a Lexmark
E260n Printer

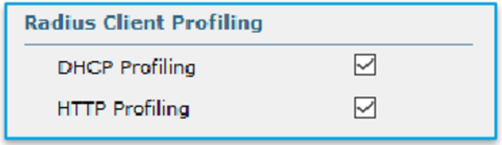

☑ RADIUS

Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP

From 15.0(2)SE

```
device-sensor accounting
device-sensor notify all-changes
```

From AireOS 7.2

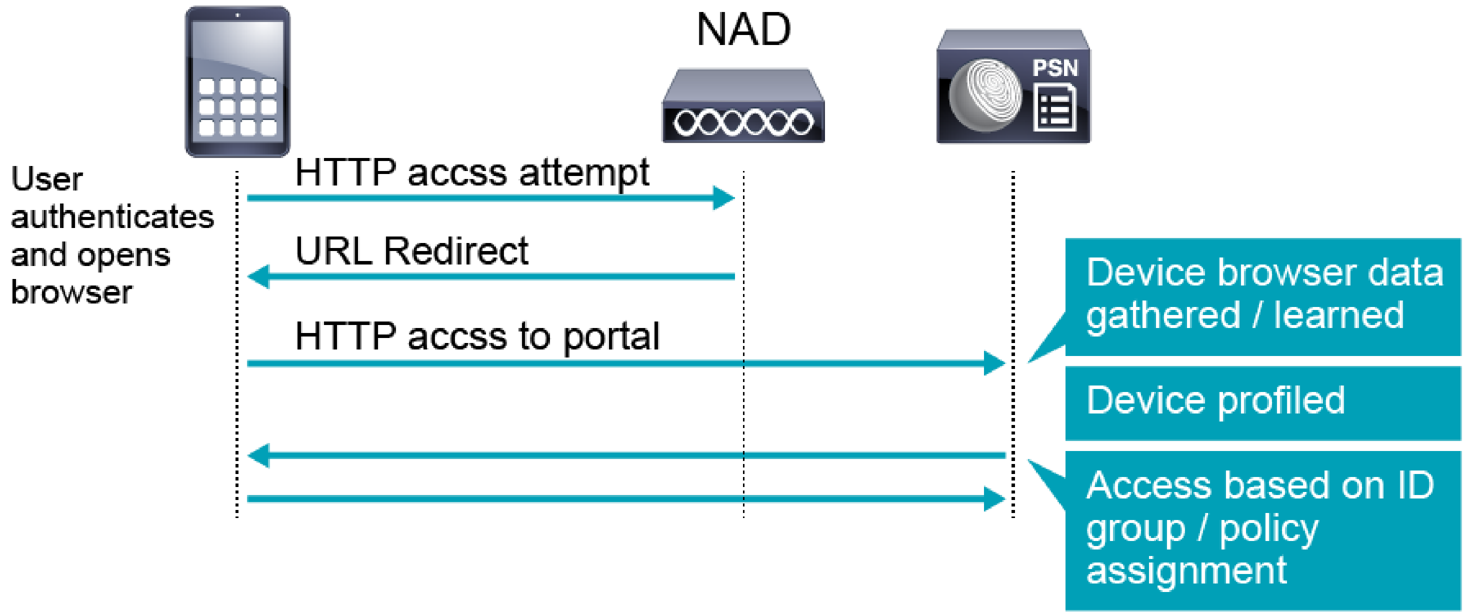

Radius Client Profiling

DHCP Profiling ☑

HTTP Profiling ☑

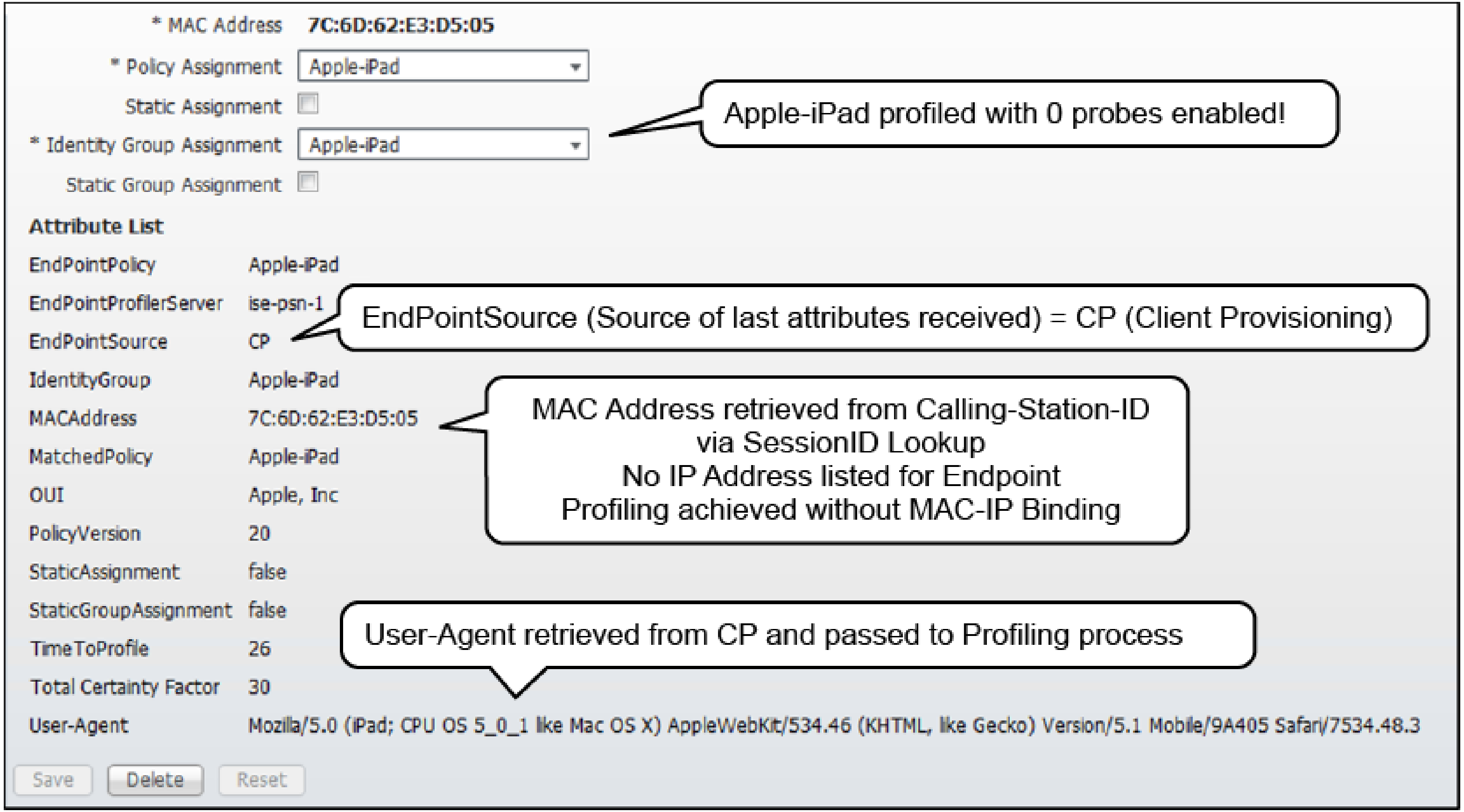
WLANs > (SSID) > Advanced

HTTP Profiling Without Probes


NAD
PSN
User authenticates and opens browser
HTTP accss attempt
URL Redirect
HTTP accss to portal
Device browser data gathered / learned
Device profiled
Access based on ID group / policy assignment

- Direct Profiling using Client Provisioning
- Client Provisioning captures user agent and MAC address from SessionID for profiling purposes

Profile Attributes Obtained Without Probes



* MAC Address 7C:6D:62:E3:D5:05

* Policy Assignment Apple-iPad

Static Assignment □

* Identity Group Assignment Apple-iPad

Static Group Assignment □

Apple-iPad profiled with 0 probes enabled!

Attribute List

EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	CP
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	26
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3

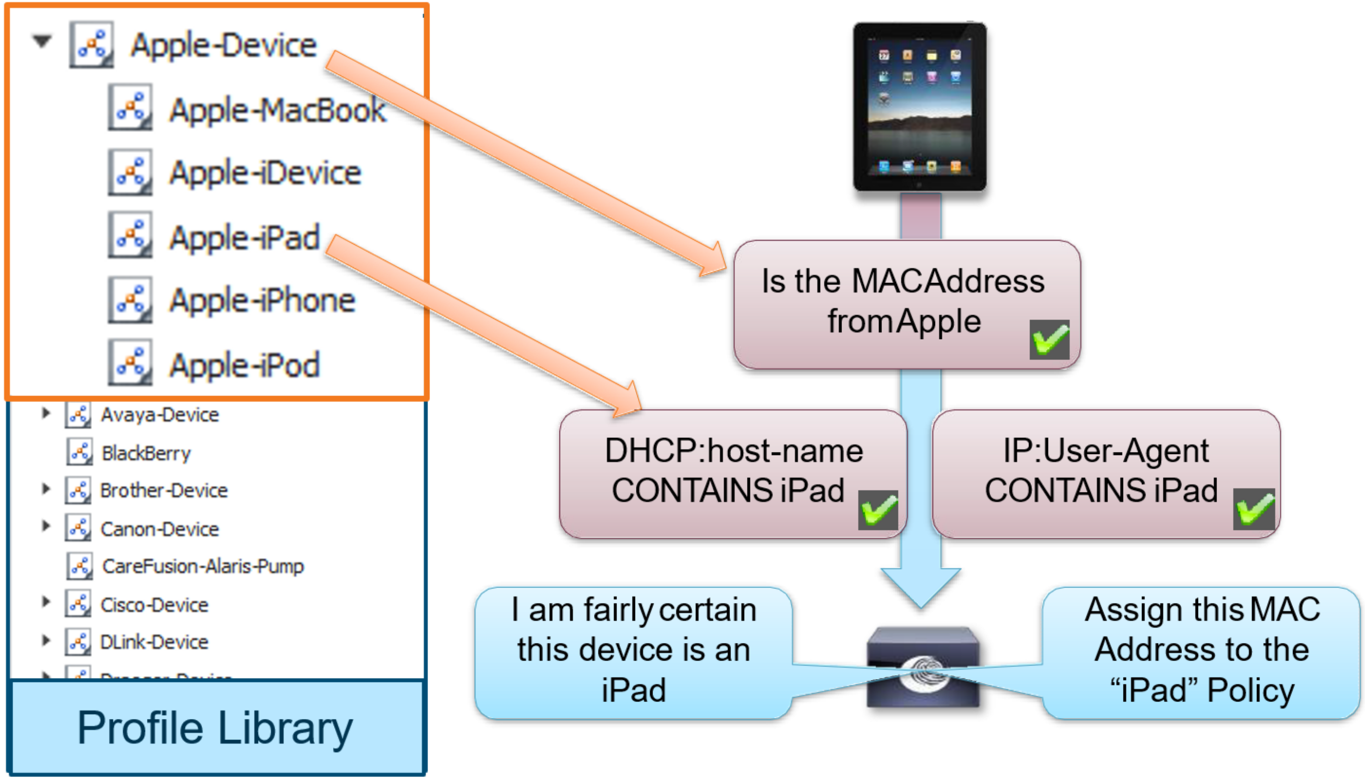
EndPointSource (Source of last attributes received) = CP (Client Provisioning)

MAC Address retrieved from Calling-Station-ID
via SessionID Lookup
No IP Address listed for Endpoint
Profiling achieved without MAC-IP Binding

User-Agent retrieved from CP and passed to Profiling process

Profiling Policy Overview

Profile Policies Use a Combination of Conditions to Identify Devices



Is the MACAddress fromApple ✓

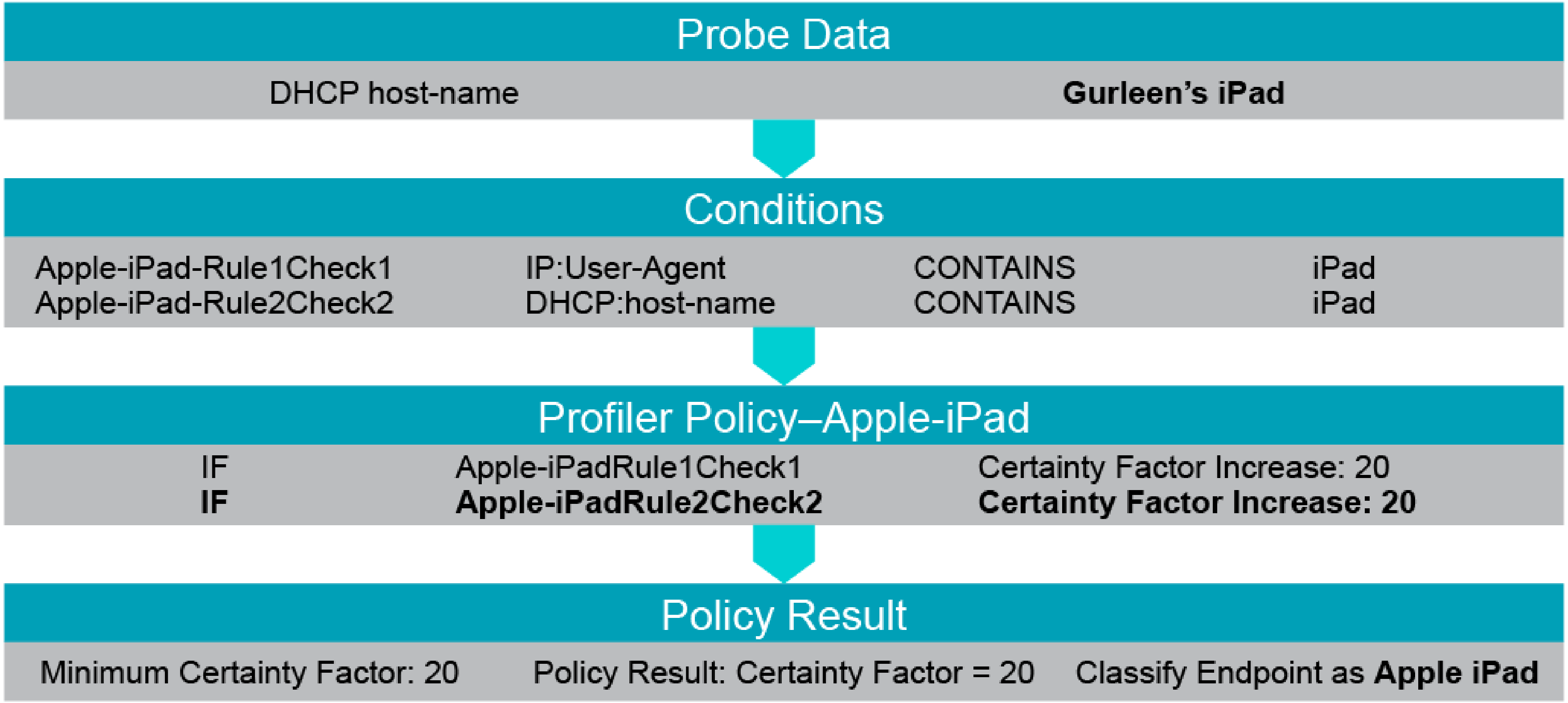
DHCP:host-name CONTAINS iPad ✓

IP:User-Agent CONTAINS iPad ✓

I am fairly certain this device is an iPad

Assign this MAC Address to the “iPad” Policy

Profiling Flow Example



Probe Data

DHCP host-name	**Gurleen’s iPad**

Conditions

Apple-iPad-Rule1Check1	IP:User-Agent	CONTAINS	iPad
Apple-iPad-Rule2Check2	DHCP:host-name	CONTAINS	iPad

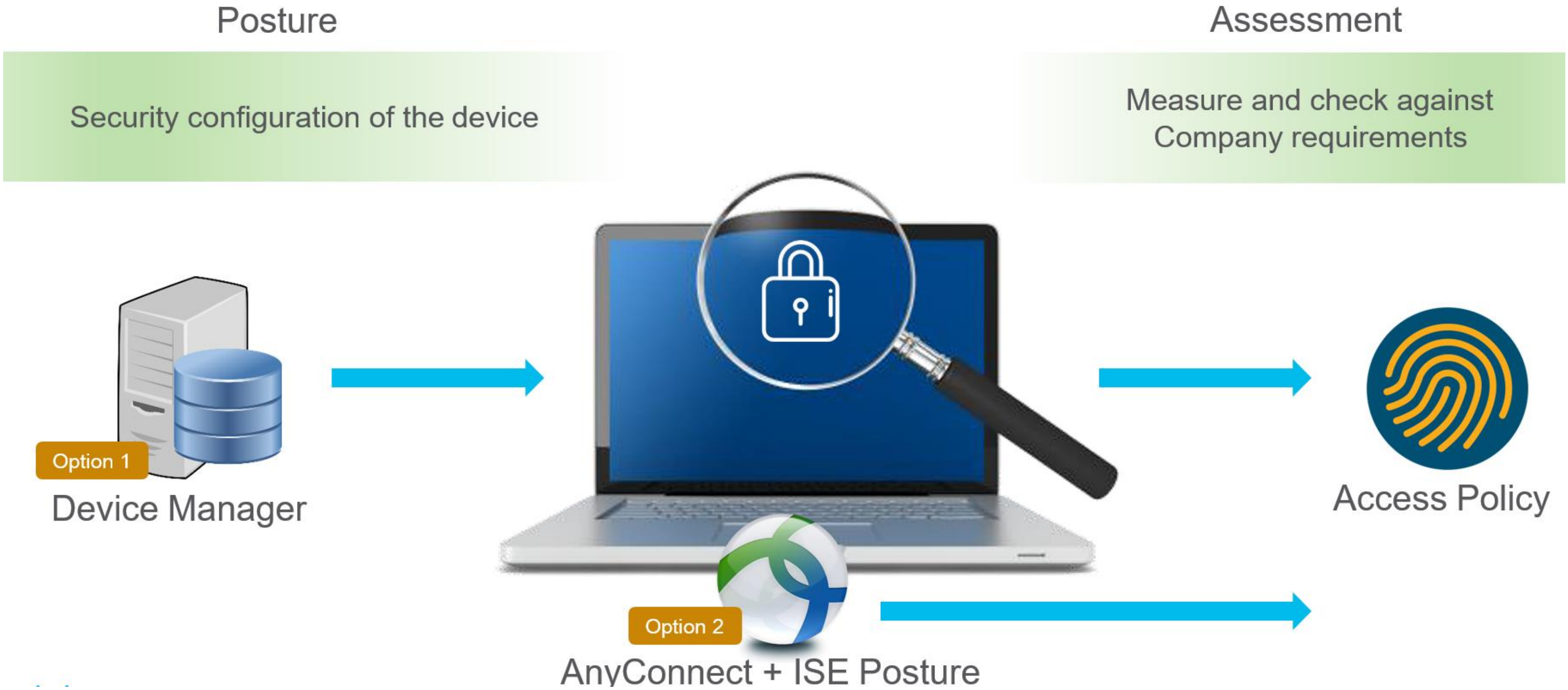
Profiler Policy–Apple-iPad

IF	Apple-iPadRule1Check1	Certainty Factor Increase: 20
IF	**Apple-iPadRule2Check2**	**Certainty Factor Increase: 20**

Policy Result

Minimum Certainty Factor: 20	Policy Result: Certainty Factor = 20	Classify Endpoint as **Apple iPad**

Проверка состояния устройств (Posture)



Posture

Security configuration of the device

Assessment

Measure and check against Company requirements

Option 1

Device Manager

Option 2

AnyConnect + ISE Posture

Access Policy

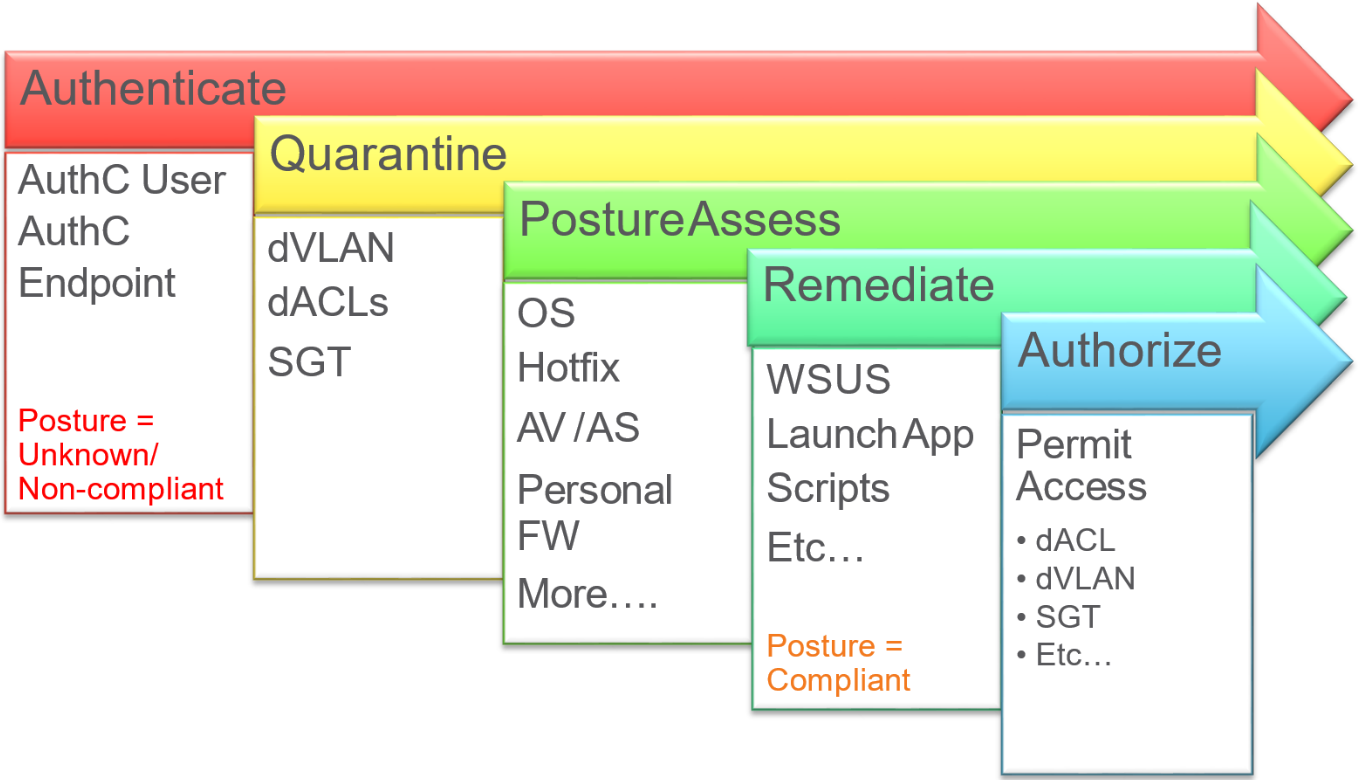
Posture: What is a Trusted Device?

1. Device Registration
2. Anti-Malware
3. Minimum OS
4. Software Patching
5. Password/Screen-lock Enforcement
6. Hardware/Software Inventory
7. Rooted Device Detection (Mobile Only)

Posture Guidelines

- Secure Enablement: Don’t stop users working
- Minimise the Impact: Avoid disrupting workflows
- Remediation: Automate and/or simplify
- Expect Complexity: There’s always something hidden!

ISE Posture Assessment

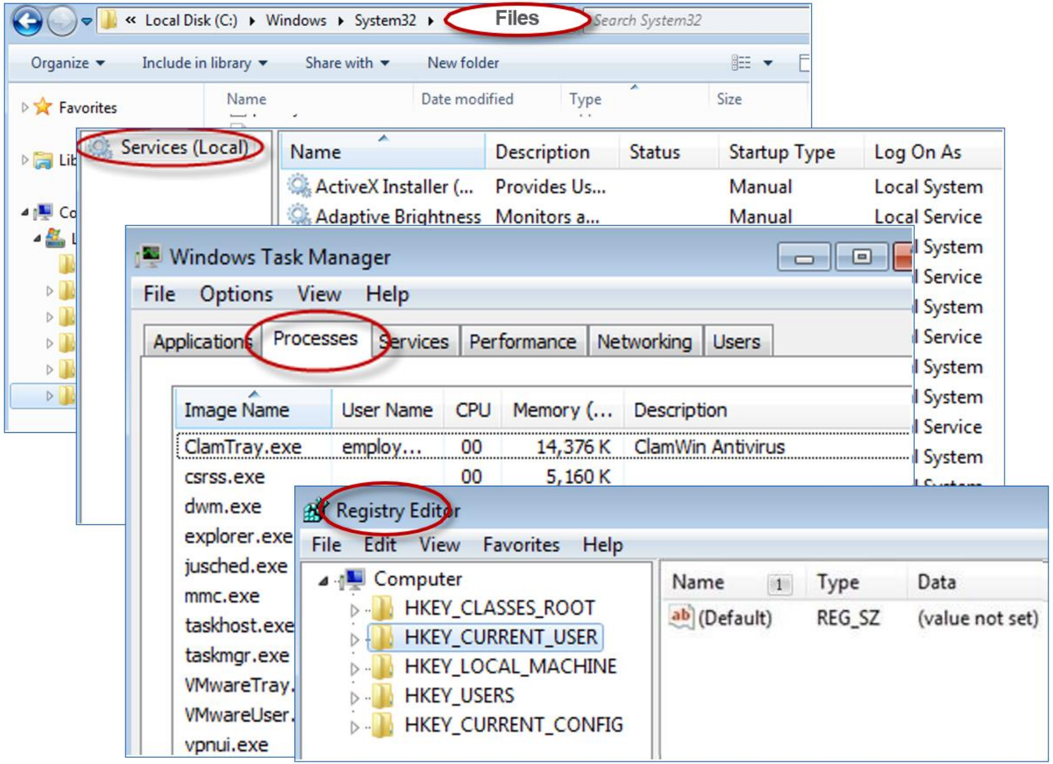


ISE Posture Assessment Checks

Microsoft Windows

Mac OS

- Microsoft Updates
  - Service Packs
  - Hotfixes
  - OS/Browser versions
- Antivirus
  - Installation/Signatures
- Antispyware
  - Installation/Signatures
- File data
- Services
- Applications/Processes
- Registry keys



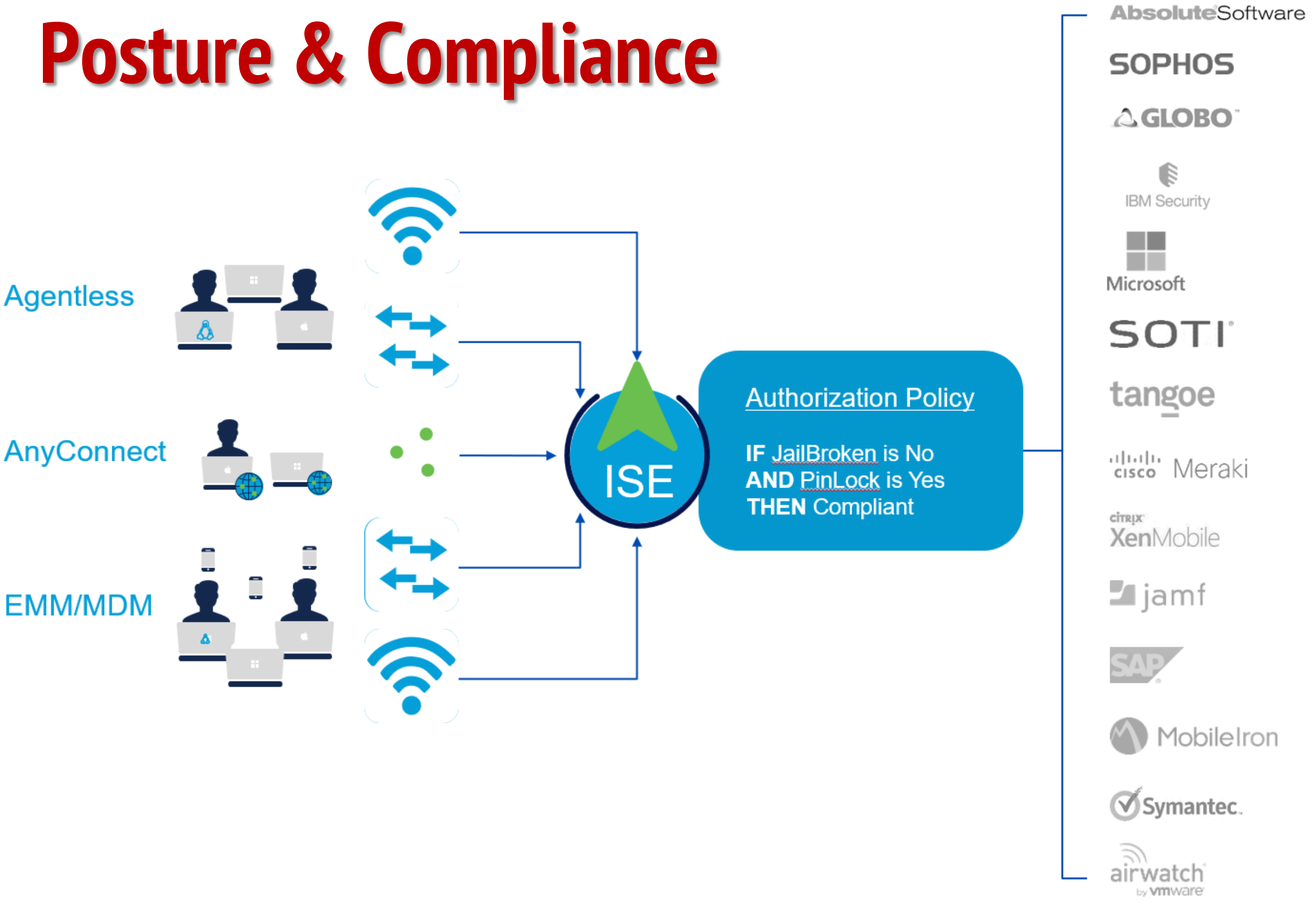
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (...	Provides Us...		Manual	Local System
Adaptive Brightness	Monitors a...		Manual	Local Service
				System
				Service
				System
				Service
				System
				System
				Service
				System

Image Name	User Name	CPU	Memory (...	Description
ClamTray.exe	employ...	00	14,376 K	ClamWin Antivirus
csrss.exe		00	5,160 K	
dwm.exe				
explorer.exe				
jusched.exe				
mmc.exe				
taskhost.exe				
taskmgr.exe				
VMwareTray.				
VMwareUser.				
vpnui.exe				

Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Name	Type	Data
(Default)	REG_SZ	(value not set)

Posture & Compliance



Authorization Policy

IF JailBroken is No
AND PinLock is Yes
THEN Compliant

MDM Attributes

ActivityType
AdminAction
AdminActionUUID
AnyConnectVersion
DaysSinceLastCheckin
DetailedInfo
DeviceID
DeviceName
DeviceType
DiskEncryption
EndPointMatchedProfile
FailureReason
IdentityGroup
IMEI
IpAddress
JailBroken
LastCheckInTimeStamp
MacAddress
Manufacturer
MDMCompliantStatus
MDMFailureReason
MDMServerName
MEID
Model
OperatingSystem
PhoneNumber
PinLock
PolicyMatched
RegisterStatus
SerialNumber
ServerType
SessionId
UDID
UserName
UserNotified

Проверка состояния устройств (Posture)

Как проверить результаты работы:

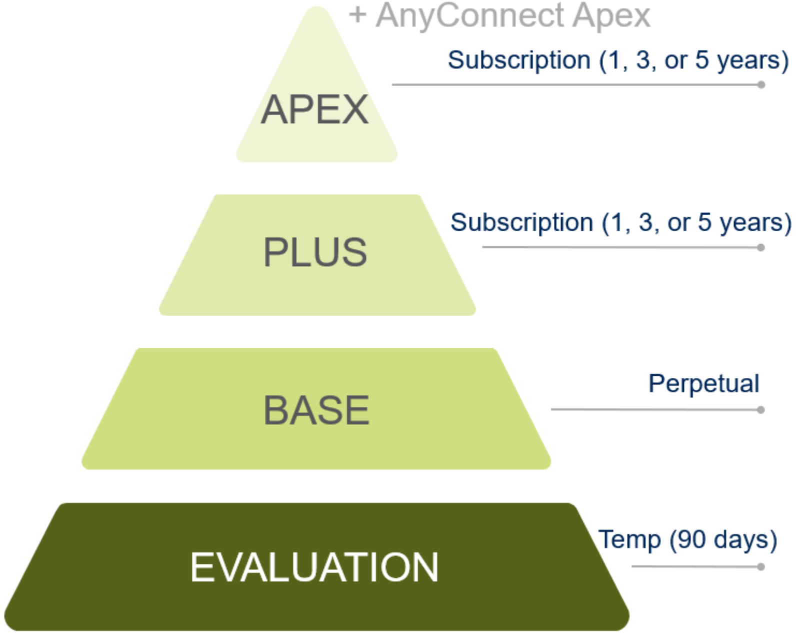
- В ISE перейти в раздел **Operations > RADIUS > Live Logs**
- В ISE перейти в раздел **Operations > Reports**. Выбрать отчет **Endpoints and Users > Posture Assessment by Condition**
- В ISE перейти в раздел **Operations > Reports**. Выбрать отчет **Endpoints and Users > Posture Assessment by Endpoint**
- Перейти в меню **Context Visibility > Endpoints > Compliance**

Дальше можно анализировать корректность и полноту настроенных политик.

Лицензирование Cisco ISE (до версии 2.7.0)

#3

- Licenses are uploaded to the Primary Administration node and propagated to the other Cisco ISE nodes in the cluster
- Base license is fundamental for use of Plus / Apex services
- License count based on concurrent endpoint sessions



+ AnyConnect Apex

APEX

Subscription (1, 3, or 5 years)

- Third Party Mobile Device Management (MDM)
- Posture Compliance
- Threat Centric NAC (TC-NAC)

PLUS

Subscription (1, 3, or 5 years)

- BYOD with built-in Certificate Authority Services
- Profiling and Feed Services
- Endpoint Protection Service (EPS)
- Cisco pxGrid

BASE

Perpetual

- Basic network access: AAA, IEEE-802.1X
- Guest management
- Easy Connect (Passive ID)
- TrustSec (SGT, SGACL, ACI Integration)
- ISE Application Programming Interfaces

EVALUATION

Temp (90 days)

- Full Cisco ISE functionality for 100 endpoints.

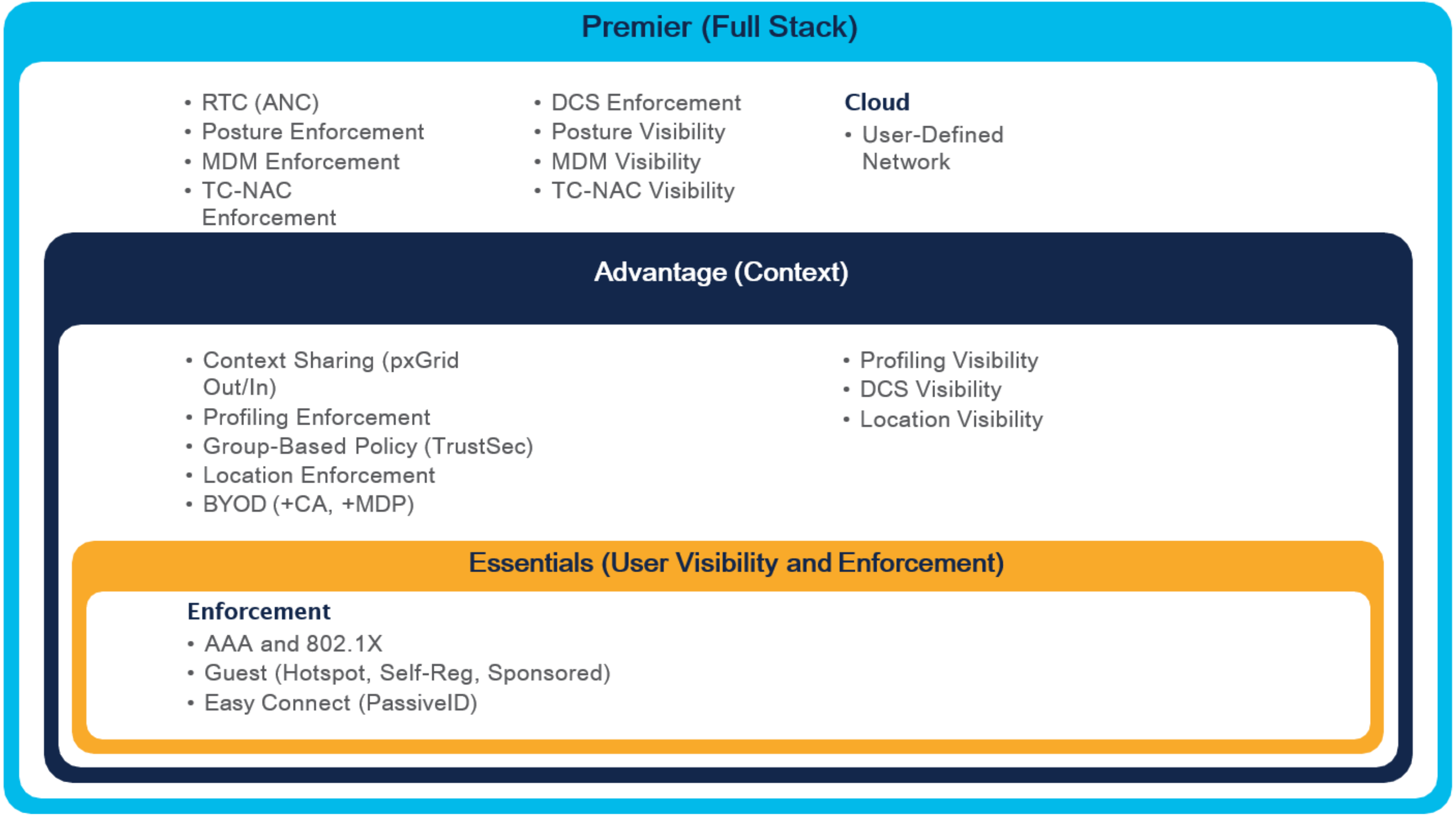
ADDITIONAL OPTIONS

DEVICE ADMIN

Perpetual

- Cisco ISE requires a Device Administration license to use the TACACS+ service on top of an existing Base or Mobility license.

Лицензирование на основании подписок (с версии 3.0.0)



Premier (Full Stack)

- RTC (ANC)
- Posture Enforcement
- MDM Enforcement
- TC-NAC Enforcement

- DCS Enforcement
- Posture Visibility
- MDM Visibility
- TC-NAC Visibility

Cloud

- User-Defined Network

Advantage (Context)

- Context Sharing (pxGrid Out/In)
- Profiling Enforcement
- Group-Based Policy (TrustSec)
- Location Enforcement
- BYOD (+CA, +MDP)

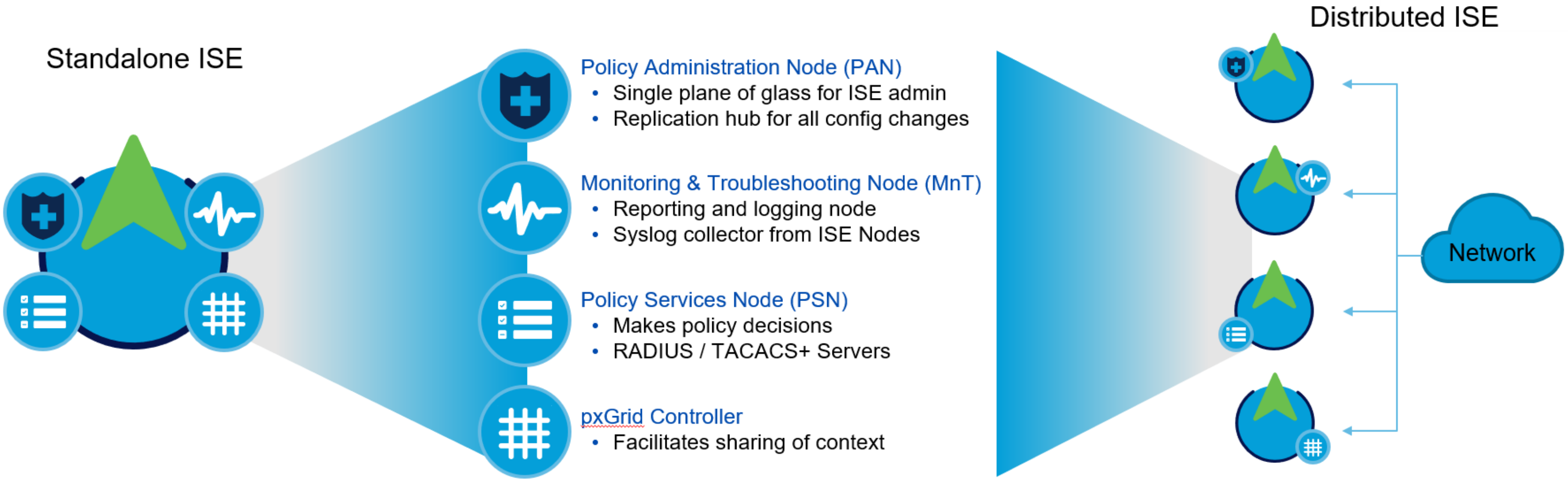
- Profiling Visibility
- DCS Visibility
- Location Visibility

Essentials (User Visibility and Enforcement)

Enforcement

- AAA and 802.1X
- Guest (Hotspot, Self-Reg, Sponsored)
- Easy Connect (PassiveID)

Архитектура Cisco ISE



Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all config changes

Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes

Policy Services Node (PSN)

- Makes policy decisions
- RADIUS / TACACS+ Servers

pxGrid Controller

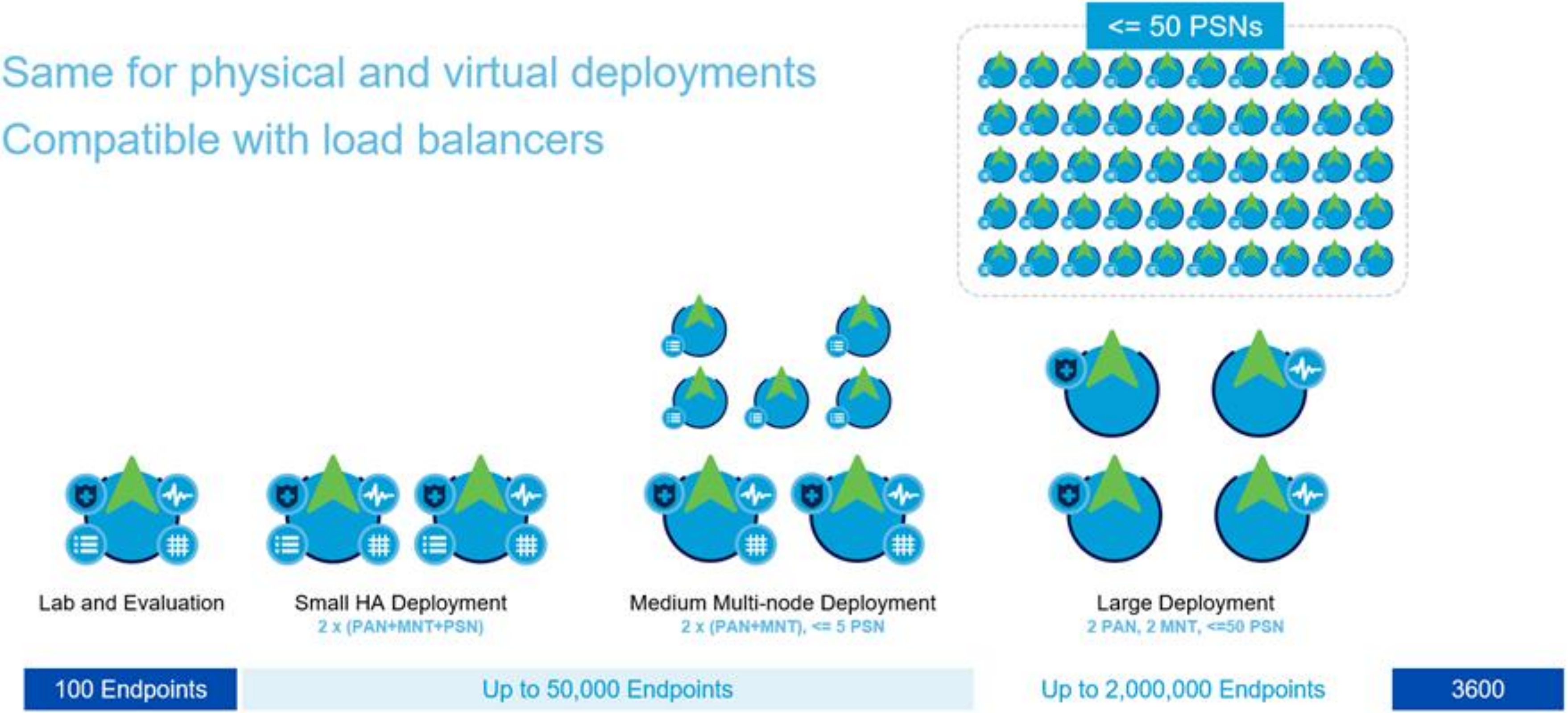
- Facilitates sharing of context

Single Node (Virtual/Appliance)		Multiple Nodes (Virtual/Appliance)
Up to **50,000** concurrent endpoints	3600	Up to **2,000,000** concurrent endpoints

Разворачивание Cisco ISE (2.6+)

Same for physical and virtual deployments

Compatible with load balancers



<= 50 PSNs

Lab and Evaluation

Small HA Deployment

2 x (PAN+MNT+PSN)

Medium Multi-node Deployment

2 x (PAN+MNT), <= 5 PSN

Large Deployment

2 PAN, 2 MNT, <=50 PSN

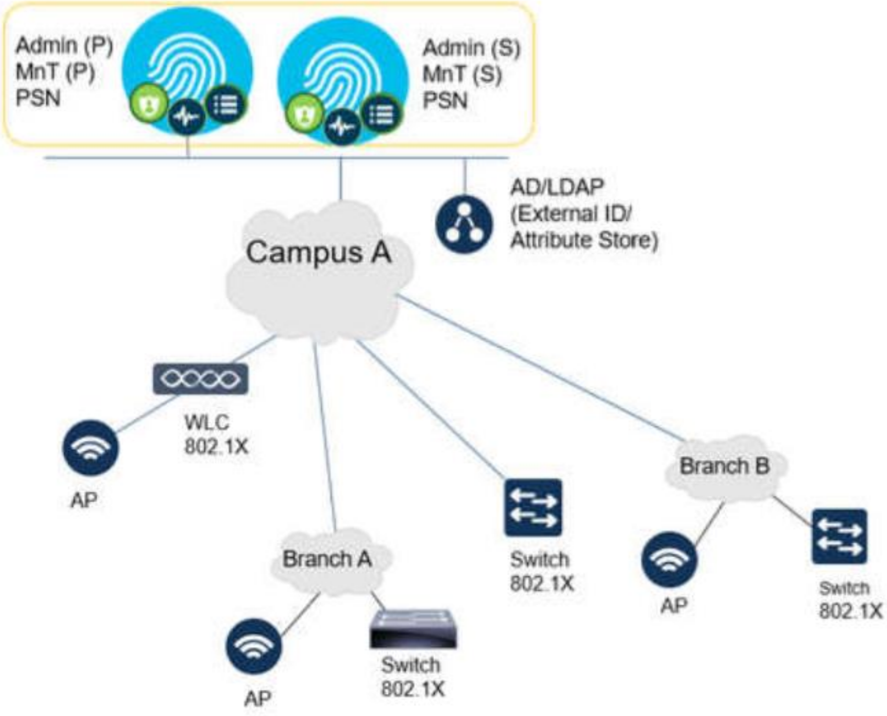
100 Endpoints

Up to 50,000 Endpoints

Up to 2,000,000 Endpoints

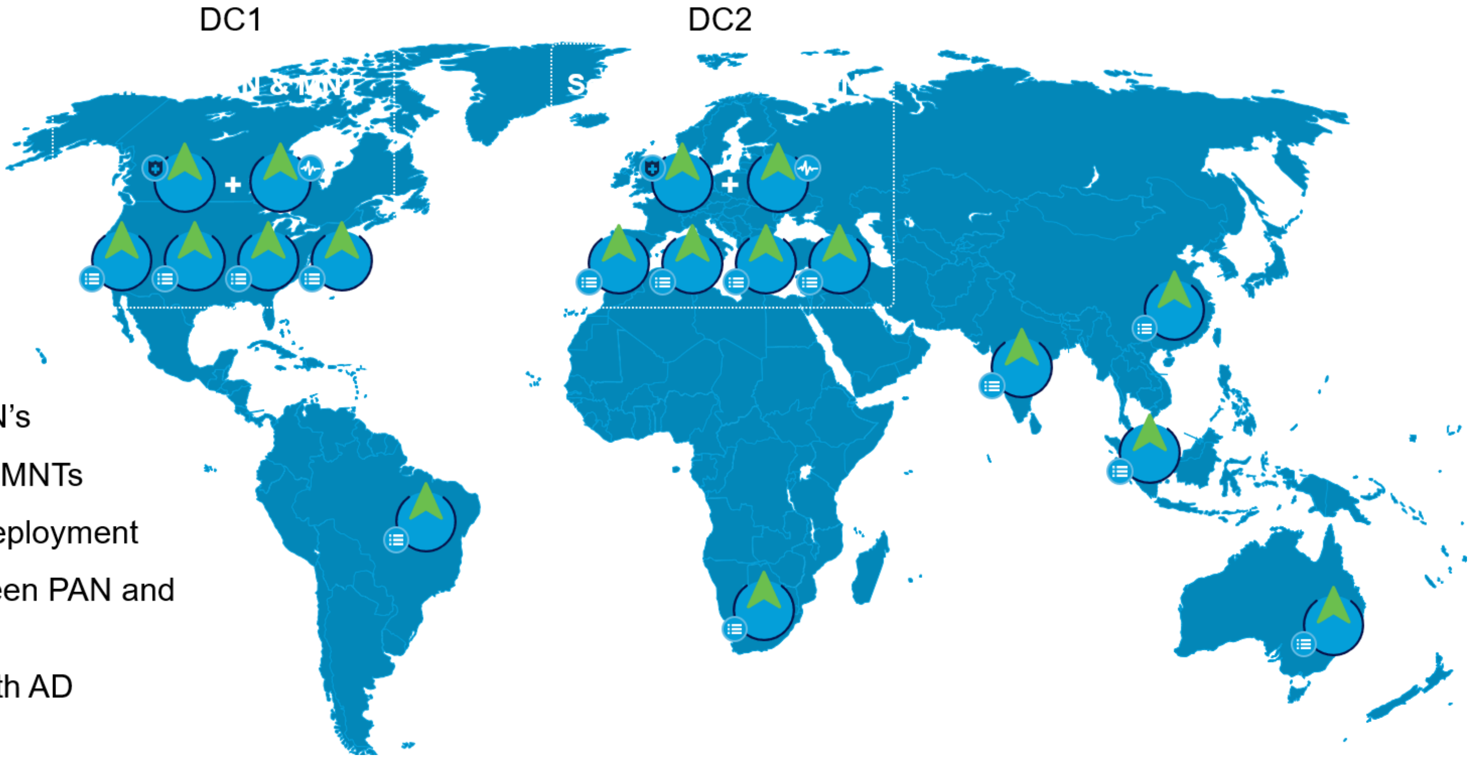
3600

In a simple 2 node ISE deployment, ISE node can have a Primary and Secondary HA pair in an active/standby mode for Administration functions and active/active pair for Monitoring functions. Policy Service is the work horse of ISE providing network access, device administration, guest access, profiling services etc. This type of deployment serves typically a single location.



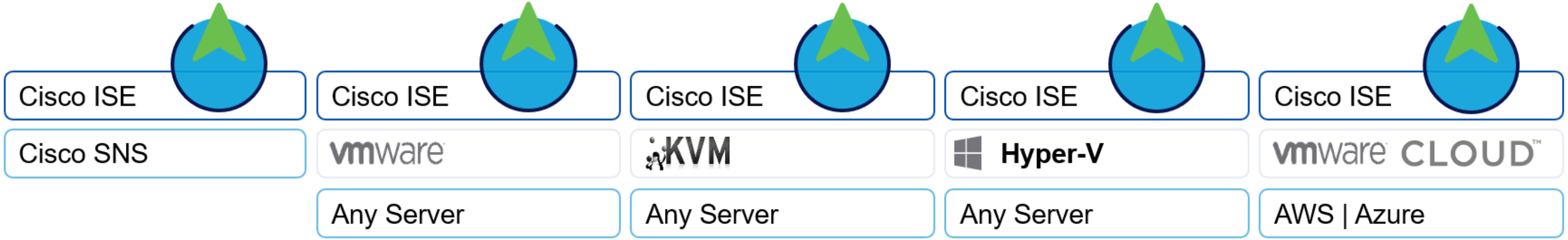
Пример построения распределенной архитектуры

- Centralize in DCs…or Distribute PSNs across Geographies



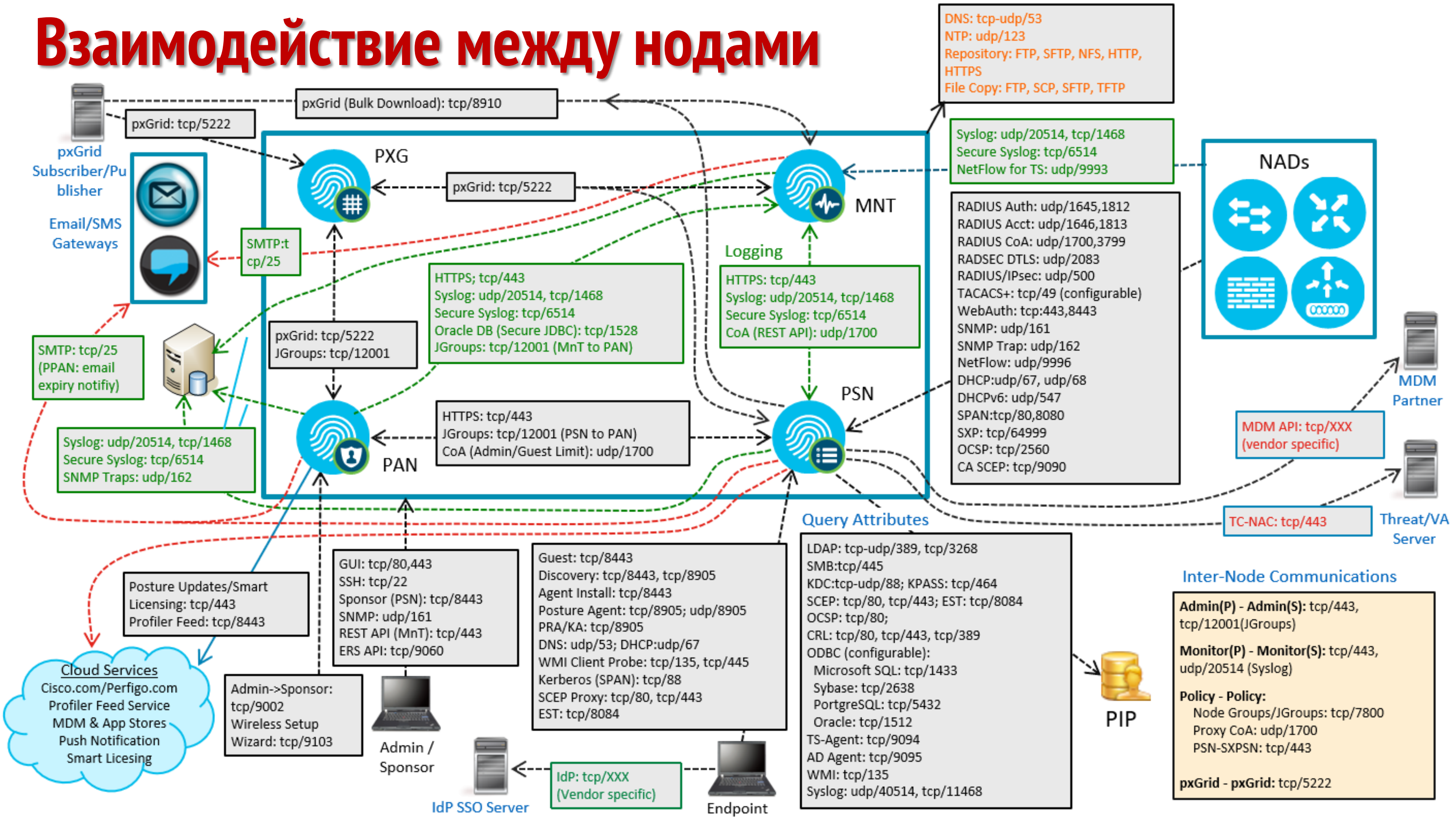
- Greater than 5 PSN’s
- Separate PAN and MNTs
- 50 PSN max per deployment
- 300ms delay between PAN and other ISE nodes
- Co-locate PSNs with AD

Поддерживаемые платформы



	Appliances	Standalone Sessions	PSN Sessions	Processor	Cores	Memory	Disk	RAID	Network Interfaces
	SNS-3615	10,000	10,000	1- intel Xeon 2.10 GHz 4110	8	32 GB (2 x 16 GB)	1 (600GB)	No	2x10Gbase-T 4x1GBase-T
	SNS-3655	25,000	50,000	1 – Intel Xeon 2.10 GHz 4116	12	96 GB (6 x 16 GB)	4 (600 GB)	10	2x10Gbase-T 4x1GBase-T
	SNS-3695	50,000	100,000	1 – Intel Xeon 2.10 GHz 4116	12	256 GB (8 x 32 GB)	8 (600 GB)	10	2x10Gbase-T 4x1GBase-T
EOL	SNS-3515	7500	7500	1 – Intel Xeon 2.40GHz E5-2620	6	16 GB (2 x 8 GB)	1 (600 GB)	NO	6x1GBase-
	SNS-3595	20,000	40,000	1 – Intel Xeon 2.60 GHz E5-2640	8	64 GB (4 x 16 GB)	4 (600 GB)	10	6x1GBase-T

Взаимодействие между нодами



DNS: tcp-udp/53
NTP: udp/123
Repository: FTP, SFTP, NFS, HTTP, HTTPS
File Copy: FTP, SCP, SFTP, TFTP

pxGrid (Bulk Download): tcp/8910

pxGrid: tcp/5222

pxGrid: tcp/5222

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
NetFlow for TS: udp/9993

SMTP:tcp/25

HTTPS; tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
Oracle DB (Secure JDBC): tcp/1528
JGroups: tcp/12001 (MnT to PAN)

HTTPS: tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
CoA (REST API): udp/1700

pxGrid: tcp/5222
JGroups: tcp/12001

SMTP: tcp/25
(PPAN: email expiry notifiy)

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
SNMP Traps: udp/162

HTTPS: tcp/443
JGroups: tcp/12001 (PSN to PAN)
CoA (Admin/Guest Limit): udp/1700

RADIUS Auth: udp/1645,1812
RADIUS Acct: udp/1646,1813
RADIUS CoA: udp/1700,3799
RADSEC DTLS: udp/2083
RADIUS/IPsec: udp/500
TACACS+: tcp/49 (configurable)
WebAuth: tcp:443,8443
SNMP: udp/161
SNMP Trap: udp/162
NetFlow: udp/9996
DHCP:udp/67, udp/68
DHCPv6: udp/547
SPAN:tcp/80,8080
SXP: tcp/64999
OCSP: tcp/2560
CA SCEP: tcp/9090

MDM API: tcp/XXX
(vendor specific)

TC-NAC: tcp/443

Posture Updates/Smart Licensing: tcp/443
Profiler Feed: tcp/8443

GUI: tcp/80,443
SSH: tcp/22
Sponsor (PSN): tcp/8443
SNMP: udp/161
REST API (MnT): tcp/443
ERS API: tcp/9060

Guest: tcp/8443
Discovery: tcp/8443, tcp/8905
Agent Install: tcp/8443
Posture Agent: tcp/8905; udp/8905
PRA/KA: tcp/8905
DNS: udp/53; DHCP:udp/67
WMI Client Probe: tcp/135, tcp/445
Kerberos (SPAN): tcp/88
SCEP Proxy: tcp/80, tcp/443
EST: tcp/8084

LDAP: tcp-udp/389, tcp/3268
SMB:tcp/445
KDC:tcp-udp/88; KPASS: tcp/464
SCEP: tcp/80, tcp/443; EST: tcp/8084
OCSP: tcp/80;
CRL: tcp/80, tcp/443, tcp/389
ODBC (configurable):
Microsoft SQL: tcp/1433
Sybase: tcp/2638
PortgreSQL: tcp/5432
Oracle: tcp/1512
TS-Agent: tcp/9094
AD Agent: tcp/9095
WMI: tcp/135
Syslog: udp/40514, tcp/11468

Cloud Services
Cisco.com/Perfigo.com
Profiler Feed Service
MDM & App Stores
Push Notification
Smart Licesing

Admin->Sponsor: tcp/9002
Wireless Setup Wizard: tcp/9103

IdP: tcp/XXX
(Vendor specific)

Inter-Node Communications

Admin(P) - Admin(S): tcp/443, tcp/12001(JGroups)

Monitor(P) - Monitor(S): tcp/443, udp/20514 (Syslog)

Policy - Policy:
Node Groups/JGroups: tcp/7800
Proxy CoA: udp/1700
PSN-SXPSN: tcp/443

pxGrid - pxGrid: tcp/5222

Подготовка к внедрению 802.1X

IT Mgr.

I've done my homework in Proof of Concept Lab and it looks good. I'm turning on 802.1X tomorrow…

Enabled 802.1X

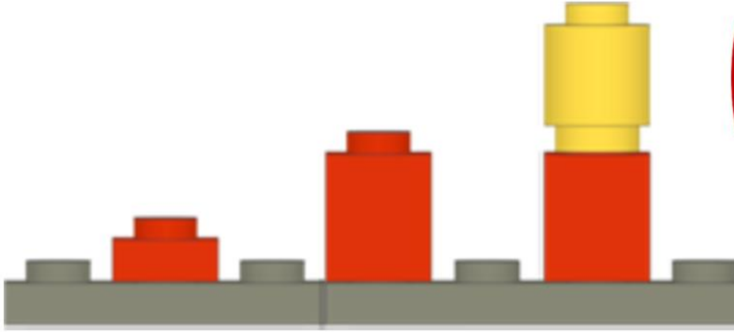
I can't connect to my network. It says Authentication failed but I don't know how to fix. My presentation is in 2 hours…

Help Desk calls increase by 40%

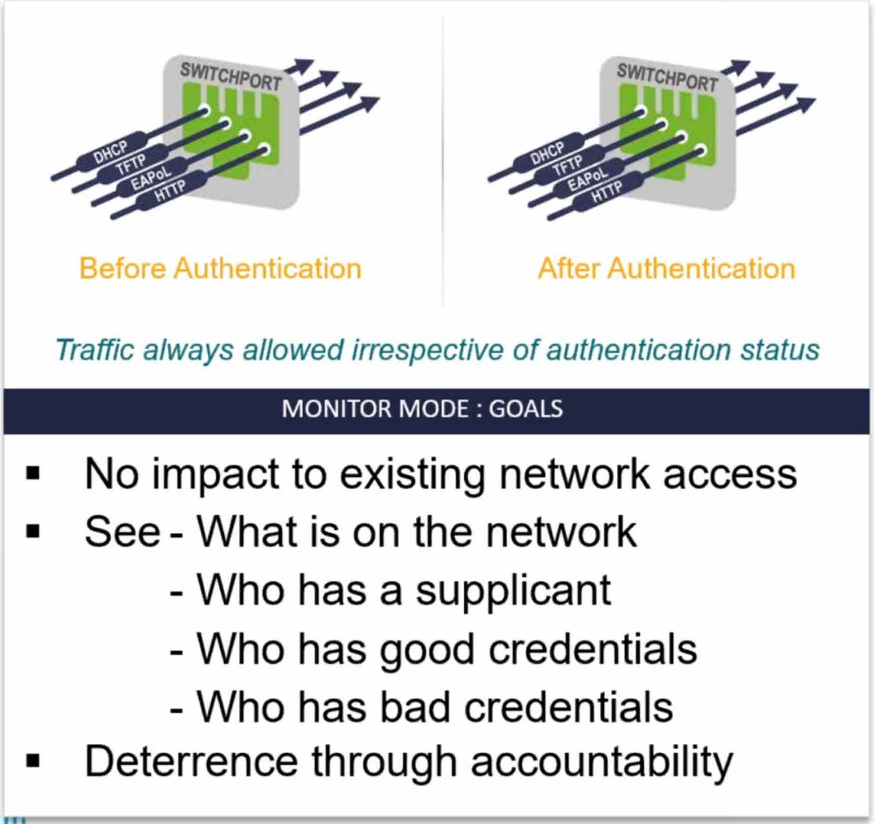
Пофазное внедрение 802.1X

- Access-Prevention Technology
  - A Monitor Mode is necessary
  - Must have ways to implement and see who will succeed and who will fail
    - Determine why, and then remediate before taking 802.1X into a stronger enforcement mode.
- Solution = Phased Approach to Deployment:
  - Monitor Mode
  - Low-Impact Mode

    -or-
  - Closed Mode



Фаза №1: Monitor Mode



Before Authentication

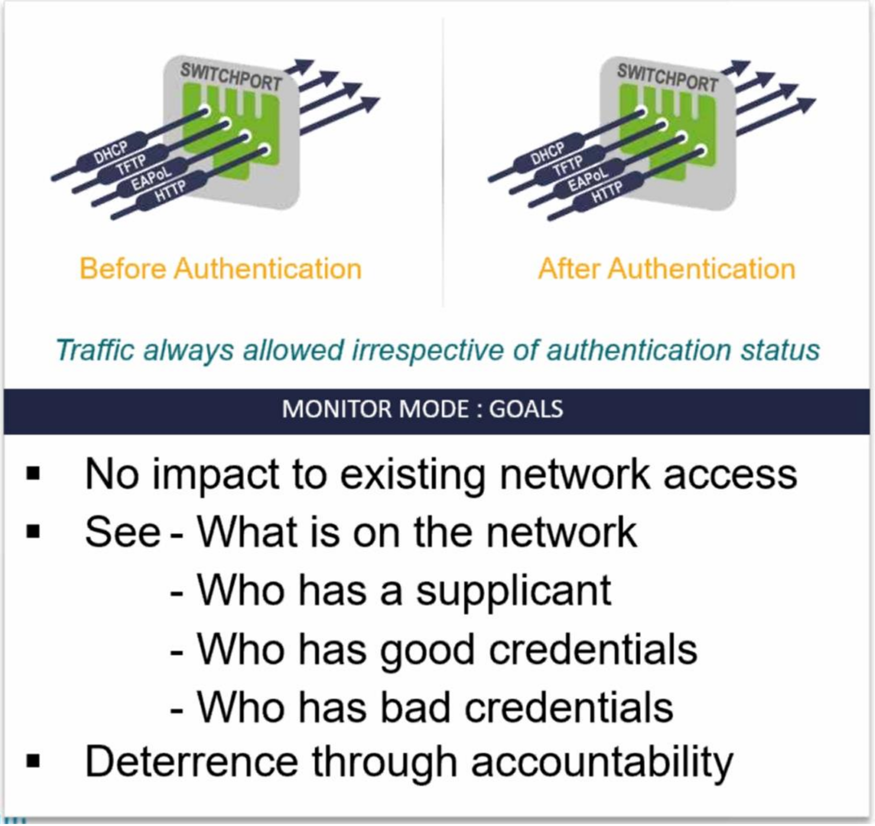
After Authentication

Traffic always allowed irrespective of authentication status

MONITOR MODE : GOALS

- No impact to existing network access
- See - What is on the network
  - Who has a supplicant
  - Who has good credentials
  - Who has bad credentials
- Deterrence through accountability

Фаза №1: Monitor Mode


SWITCHPORT
DHCP
TFTP
EAPoL
HTTP
SWITCHPORT
DHCP
TFTP
EAPoL
HTTP

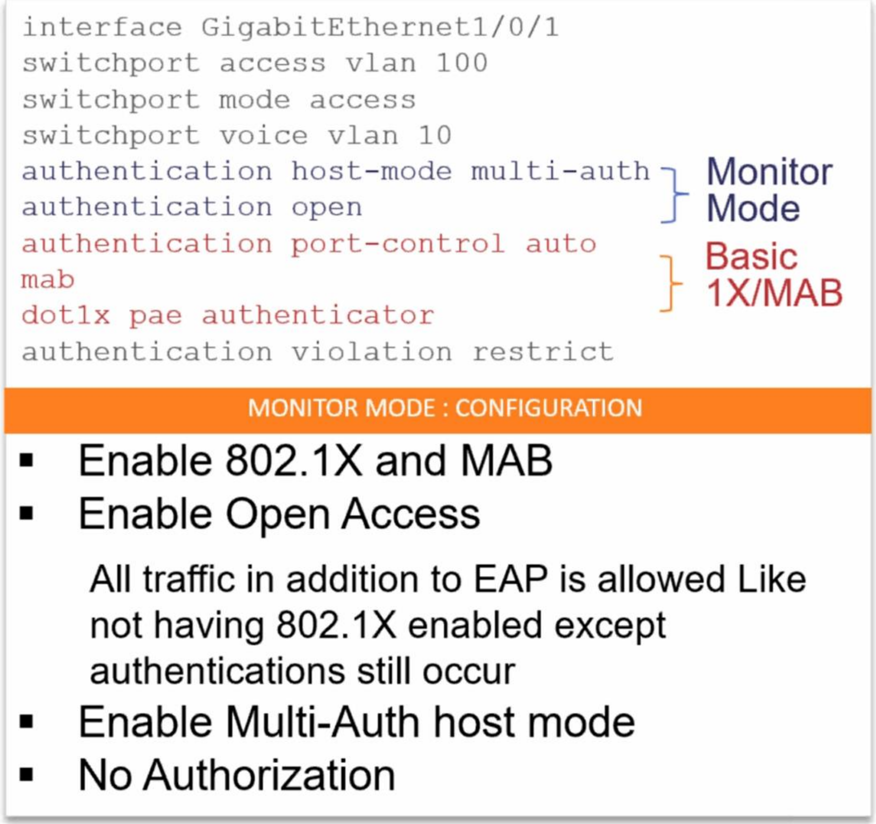
Before Authentication

After Authentication

Traffic always allowed irrespective of authentication status

MONITOR MODE : GOALS

- No impact to existing network access
- See - What is on the network
  - Who has a supplicant
  - Who has good credentials
  - Who has bad credentials
- Deterrence through accountability



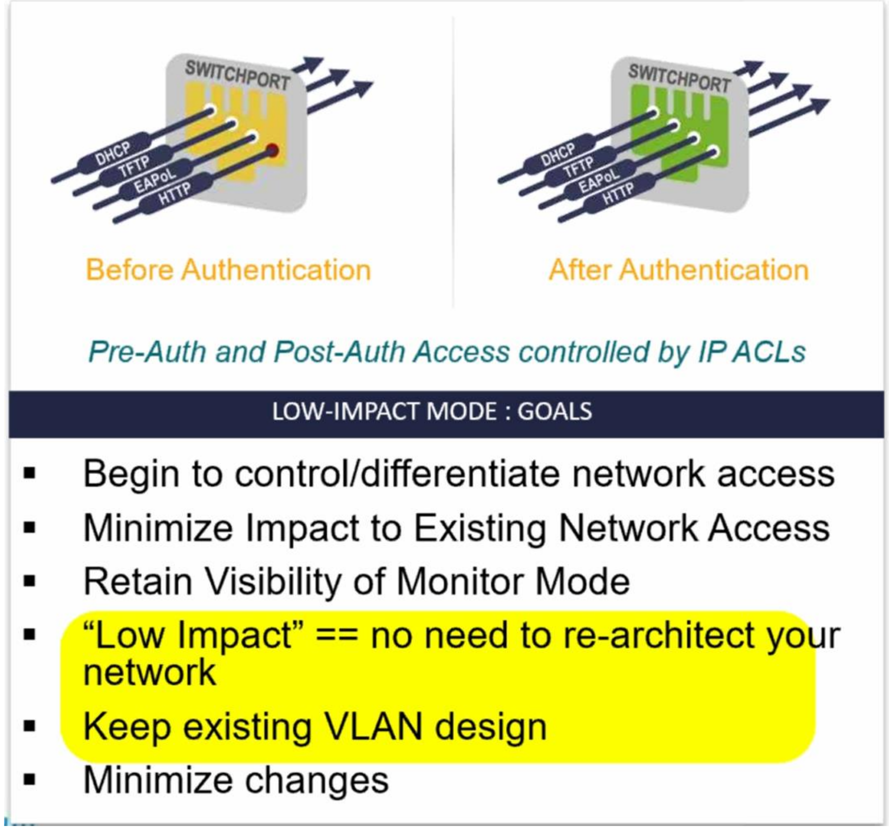
```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth ┐ Monitor
authentication open                  ┘ Mode
authentication port-control auto     ┐ Basic
mab                                  │ 1X/MAB
dot1x pae authenticator              ┘
authentication violation restrict
```

MONITOR MODE : CONFIGURATION

- Enable 802.1X and MAB
- Enable Open Access

  All traffic in addition to EAP is allowed Like not having 802.1X enabled except authentications still occur
- Enable Multi-Auth host mode
- No Authorization

Фаза №2: Low Impact Mode


SWITCHPORT
DHCP
TFTP
EAPoL
HTTP
SWITCHPORT
DHCP
TFTP
EAPoL
HTTP

Before Authentication

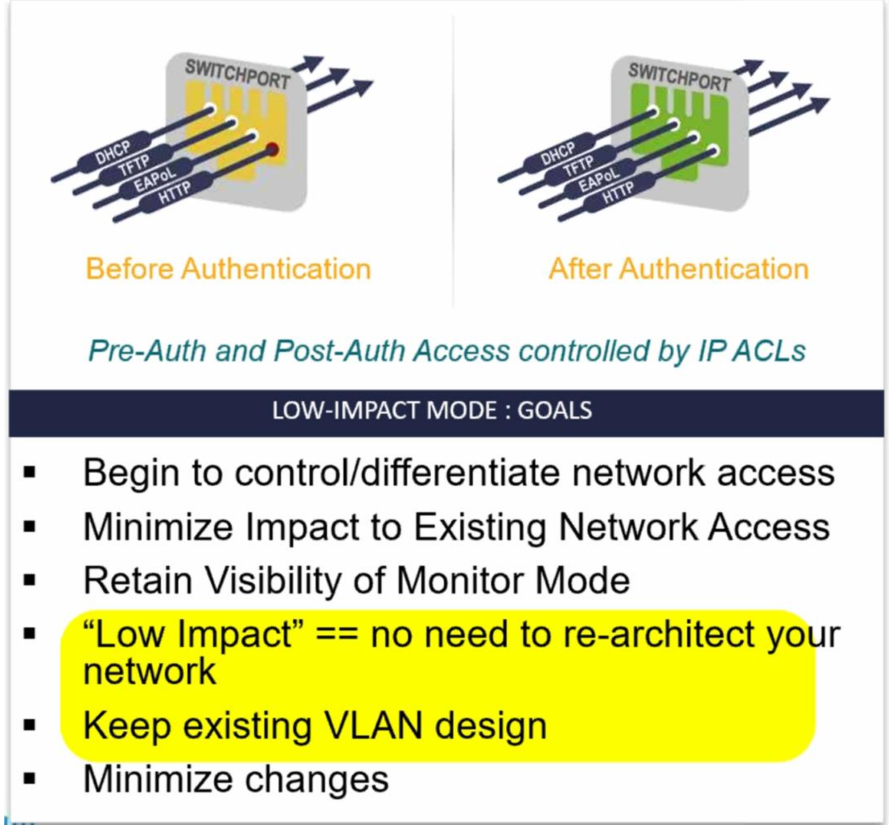
After Authentication

Pre-Auth and Post-Auth Access controlled by IP ACLs

LOW-IMPACT MODE : GOALS

- Begin to control/differentiate network access
- Minimize Impact to Existing Network Access
- Retain Visibility of Monitor Mode
- “Low Impact” == no need to re-architect your network
- Keep existing VLAN design
- Minimize changes

Фаза №2: Low Impact Mode



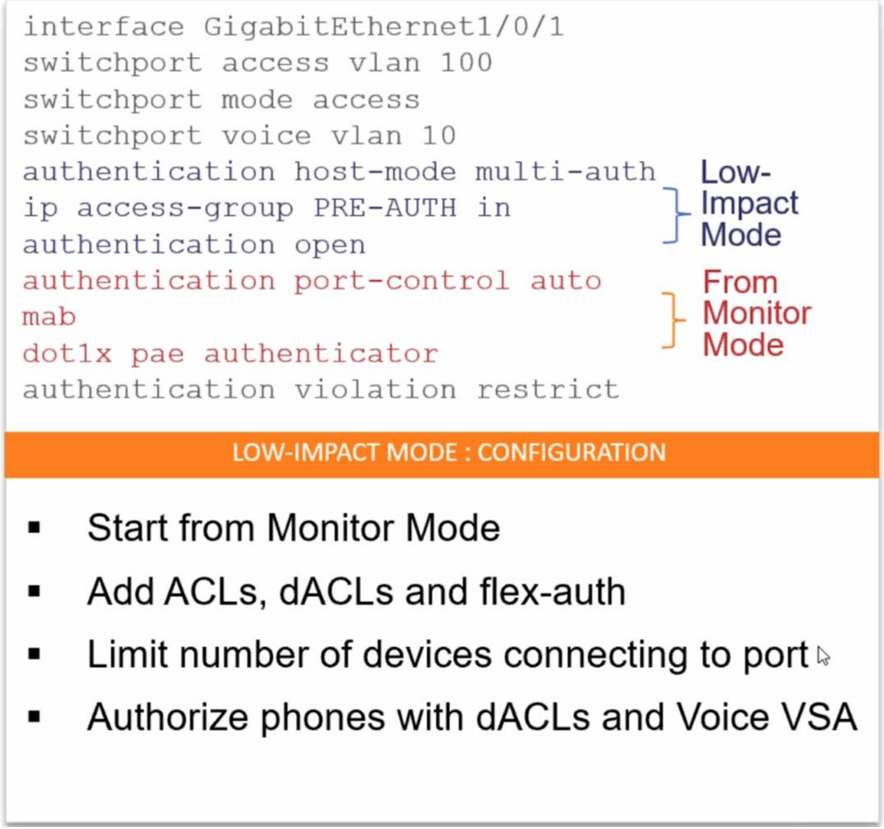
Before Authentication

After Authentication

Pre-Auth and Post-Auth Access controlled by IP ACLs

LOW-IMPACT MODE : GOALS

- Begin to control/differentiate network access
- Minimize Impact to Existing Network Access
- Retain Visibility of Monitor Mode
- “Low Impact” == no need to re-architect your network
- Keep existing VLAN design
- Minimize changes



```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth
ip access-group PRE-AUTH in
authentication open
authentication port-control auto
mab
dot1x pae authenticator
authentication violation restrict
```

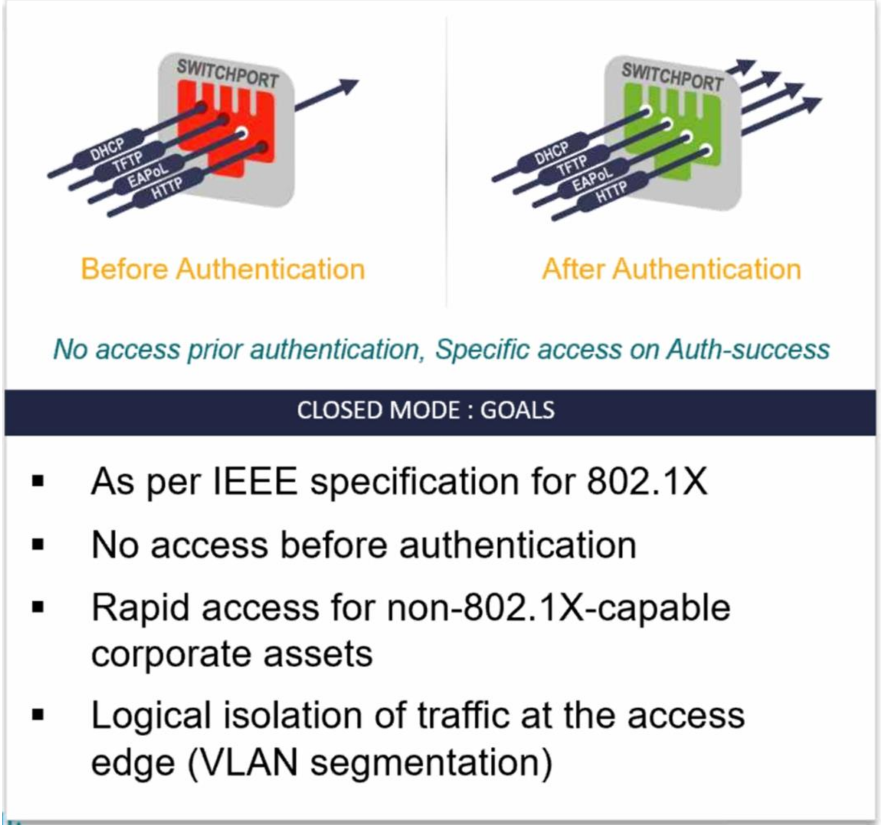
Low-Impact Mode

From Monitor Mode

LOW-IMPACT MODE : CONFIGURATION

- Start from Monitor Mode
- Add ACLs, dACLs and flex-auth
- Limit number of devices connecting to port
- Authorize phones with dACLs and Voice VSA

Фаза №3: Closed Mode



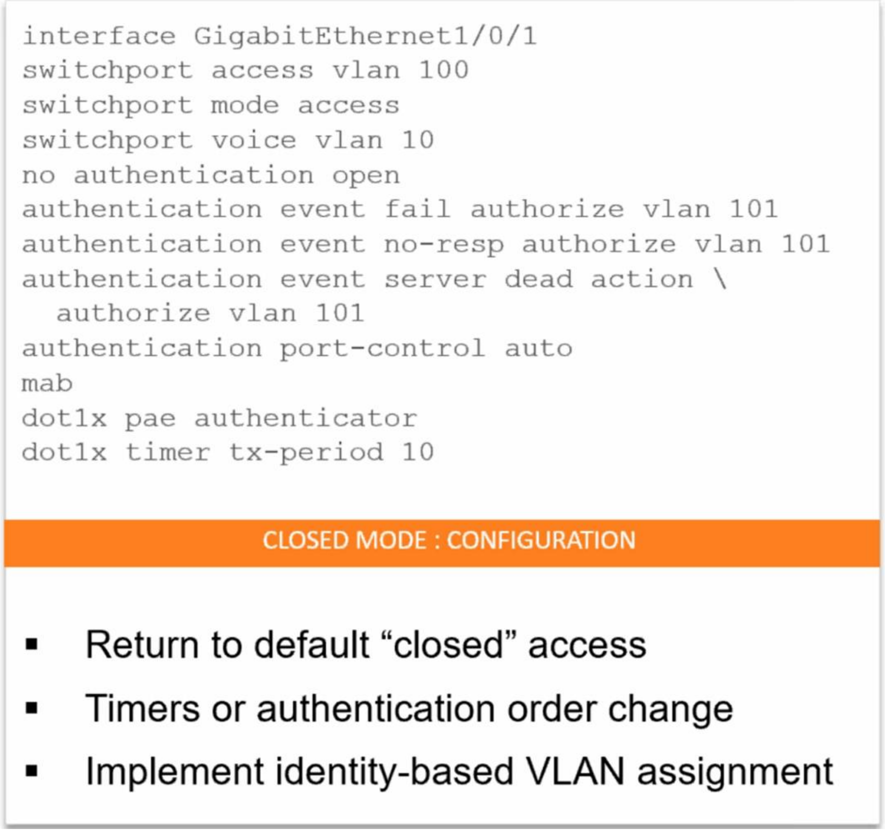
Before Authentication

After Authentication

No access prior authentication, Specific access on Auth-success

CLOSED MODE : GOALS

- As per IEEE specification for 802.1X
- No access before authentication
- Rapid access for non-802.1X-capable corporate assets
- Logical isolation of traffic at the access edge (VLAN segmentation)

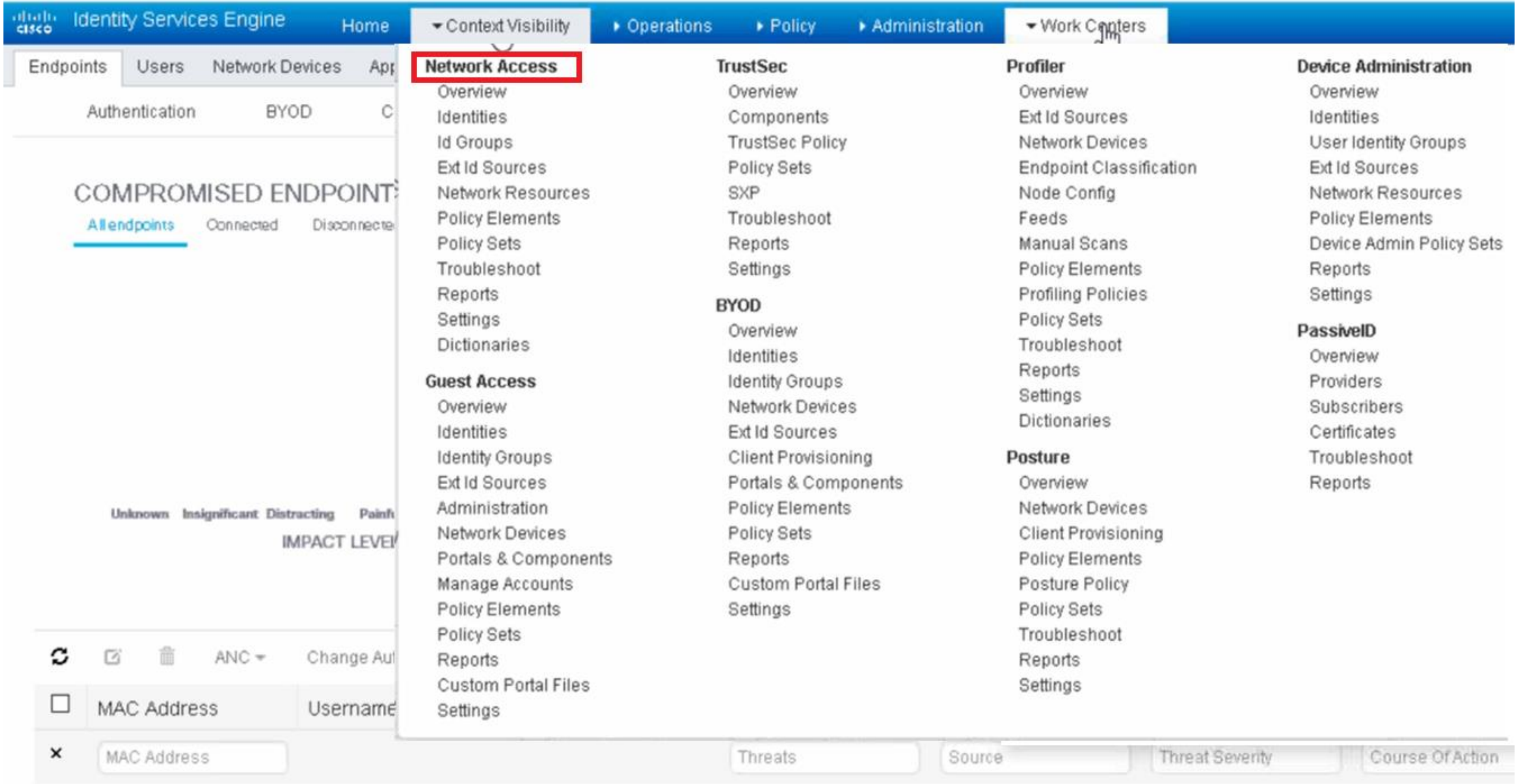


```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
no authentication open
authentication event fail authorize vlan 101
authentication event no-resp authorize vlan 101
authentication event server dead action \
  authorize vlan 101
authentication port-control auto
mab
dot1x pae authenticator
dot1x timer tx-period 10
```

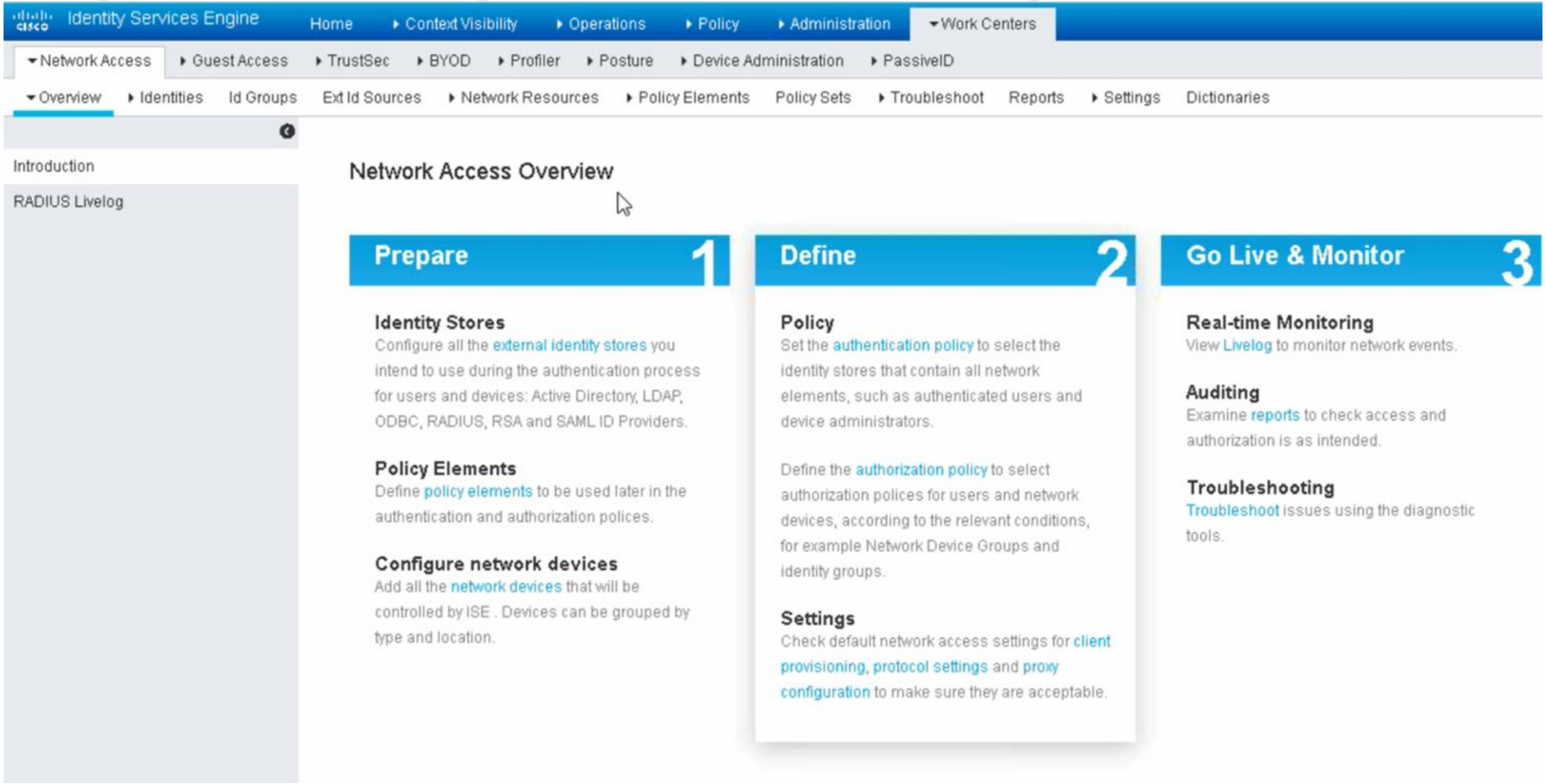
CLOSED MODE : CONFIGURATION

- Return to default “closed” access
- Timers or authentication order change
- Implement identity-based VLAN assignment

Встроенные алгоритмы выполнения рабочих задач



Встроенные алгоритмы выполнения рабочих задач



Network Access Overview

Prepare 1

Identity Stores
Configure all the external identity stores you intend to use during the authentication process for users and devices: Active Directory, LDAP, ODBC, RADIUS, RSA and SAML ID Providers.

Policy Elements
Define policy elements to be used later in the authentication and authorization polices.

Configure network devices
Add all the network devices that will be controlled by ISE . Devices can be grouped by type and location.

Define 2

Policy
Set the authentication policy to select the identity stores that contain all network elements, such as authenticated users and device administrators.

Define the authorization policy to select authorization polices for users and network devices, according to the relevant conditions, for example Network Device Groups and identity groups.

Settings
Check default network access settings for client provisioning, protocol settings and proxy configuration to make sure they are acceptable.

Go Live & Monitor 3

Real-time Monitoring
View Livelog to monitor network events.

Auditing
Examine reports to check access and authorization is as intended.

Troubleshooting
Troubleshoot issues using the diagnostic tools.

Planning & Pre-Deployment Checklists #4

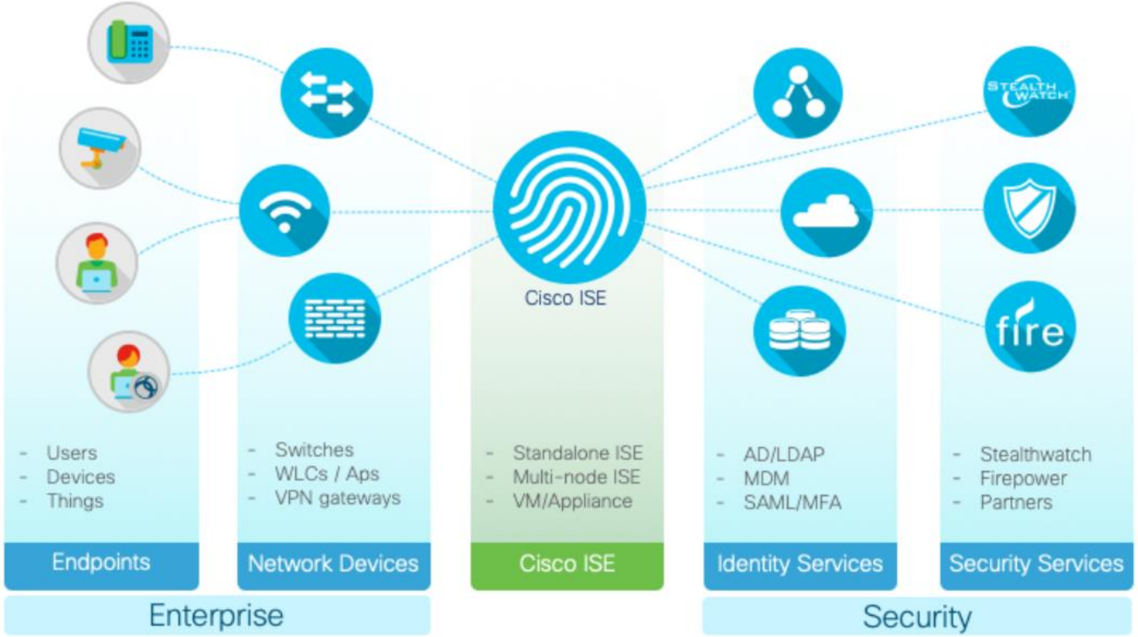
- Planning Checklists
  - Business Objectives
  - Organizational
  - Security Policy Creation and Maintenance
  - Scale
  - Public Key Infrastructure (PKI)
  - Directory Services
  - Network Access Devices (NADs)
  - Managed Endpoints
  - Assets
  - Cisco Identity Services Engine (ISE)
  - Guest Services
  - Monitoring, Reporting, and Troubleshooting
  - Communications
  - Support Desk

- Deployment Checklists
  - Network Services
  - Digital Certificates
  - Network Devices
  - Security Policy
  - Enforcement States
  - Endpoints
  - Test Scenarios

community.cisco.com/t5/security-documents/ise-planning-amp-pre-deployment-checklists/ta-p/3622635

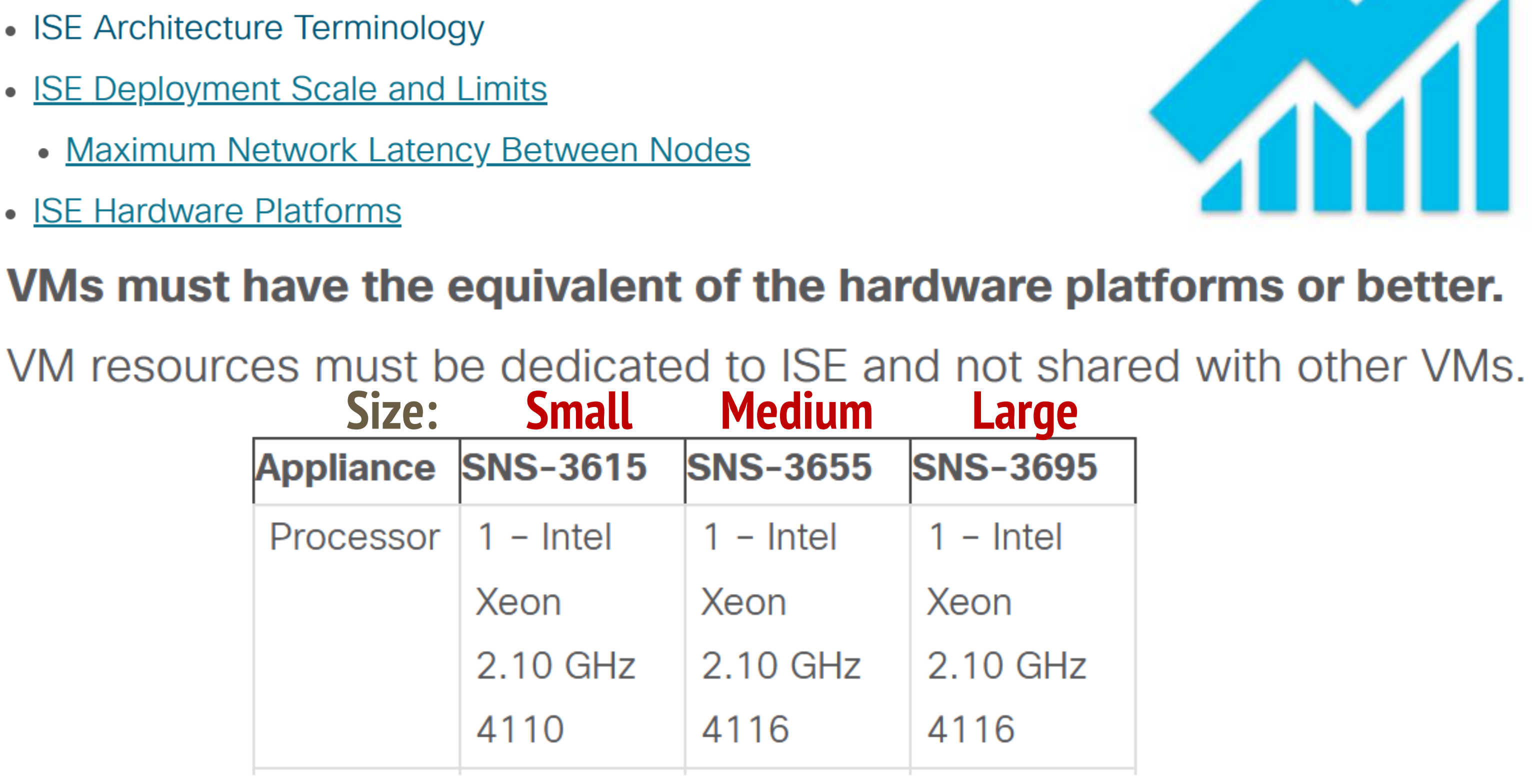
ISE High Level Design (HLD)

An ISE High Level Design (HLD) is recommended to assist you with the design and planning of your ISE deployment. Having a clearly written security policy - whether aspirational or active - is the first step in assessing, planning and deploying network access security. Without this, it is hard to break down the deployment into phases by location or capabilities. When seeking outside help, the HLD provides a huge time savings for education other teams, partners, Cisco Sales representative, Technical Assistance Center (TAC) representative or even the ISE product and engineering teams. Clearly state the desired solution capabilities, hardware and software environment and integrations can quickly allow people to understand what you want and how to configure it or troubleshoot it.



community.cisco.com/t5/security-documents/ise-high-level-design-hld/ta-p/3657418

ISE Performance & Scale



- ISE Architecture Terminology
- ISE Deployment Scale and Limits
  - Maximum Network Latency Between Nodes
- ISE Hardware Platforms

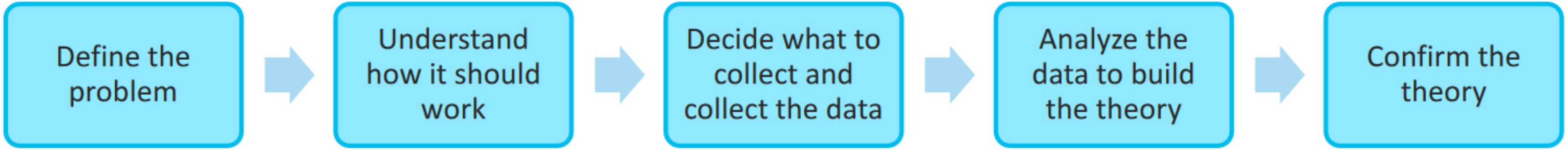
VMs must have the equivalent of the hardware platforms or better.

VM resources must be dedicated to ISE and not shared with other VMs.

Size:	Small	Medium	Large
Appliance	**SNS-3615**	**SNS-3655**	**SNS-3695**
Processor	1 – Intel Xeon 2.10 GHz 4110	1 – Intel Xeon 2.10 GHz 4116	1 – Intel Xeon 2.10 GHz 4116

community.cisco.com/t5/security-documents/ise-performance-amp-scale/ta-p/3642148

How to troubleshoot ISE



Define the problem

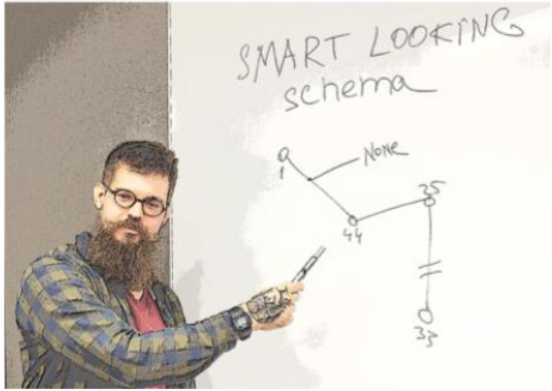
Understand how it should work

Decide what to collect and collect the data

Analyze the data to build the theory

Confirm the theory

Troubleshooting Methodology



www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKSEC-3229.pdf

Why We Buy ISE

ISE

Device Administration	TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices
Secure Access	Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use RADIUS with 802.1X, MAB, Easy Connect, or Passive ID
Guest Access	Differentiate between Corporate and Guest users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options
Asset Visibility	Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with Device Profiling. Automate access for many different IoT devices
Compliance & Posture	Use agentless posture, AnyConnect, MDM, or EMM to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access
Context Exchange	pxGrid is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase Network Visibility and facilitate automated Enforcement.
Segmentation	Group-based Policy allows for segmentation of the network through the use of Scalable Group Tags (SGT) and Scalable Group ACLs (SGACL) instead of VLAN/ACL segmentation.
Cisco SDA/DNAC	ISE integrates with DNA Center to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)
BYOD	Allow employees to use their own devices to access network resources by registering their device and downloading certificates for authentication through a simple onboarding process
Threat Containment	Using a Threat Analysis tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results

cisco Partner
Distribution Partner

ЛАН СИСТЕМС

MUK
Classics of distribution

Спасибо за внимание!

Сергей ГАЩЕНКО

sha@lansys.com.ua