



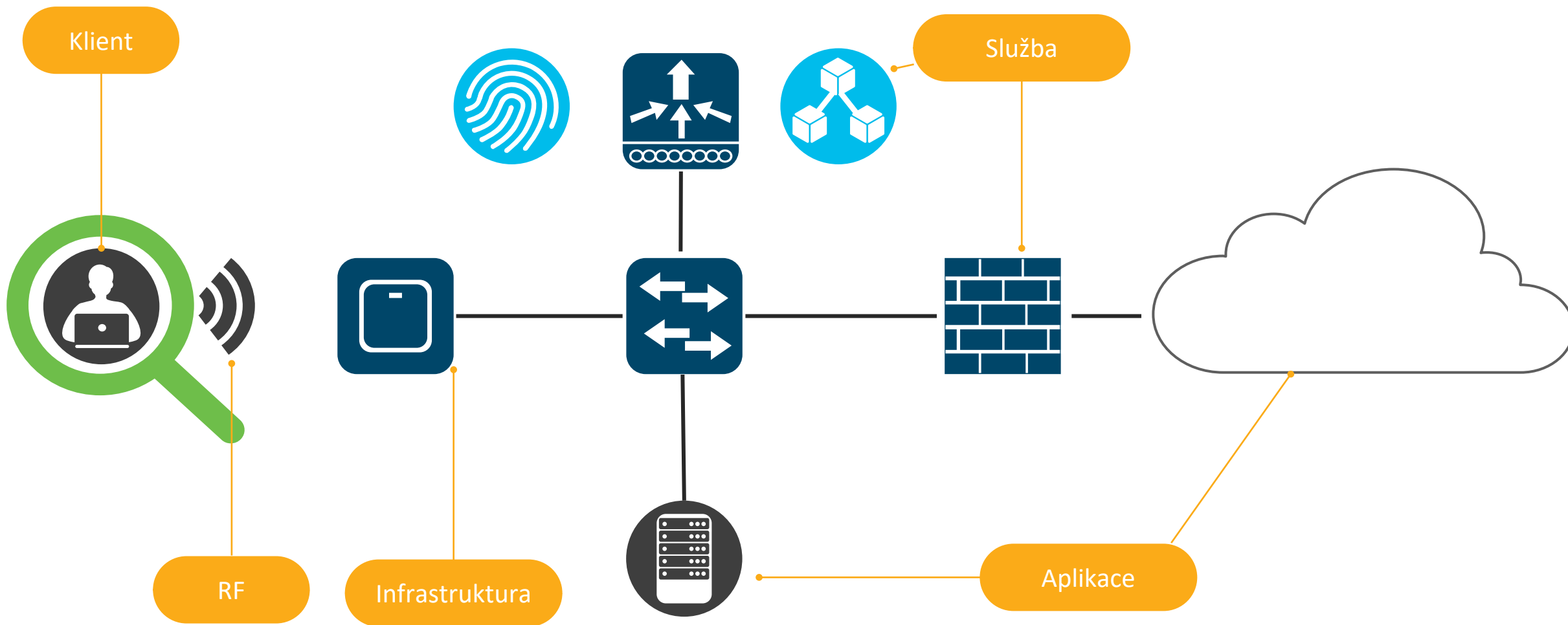
# Je Vaše Wi-Fi dostatečně zabezpečená?

Dominik Soukup – Wireless TSS

Jaroslav Čížek – CX CSS

17.1.2023

# Bezpečnost Wi-Fi sítě je komplexní otázka



# Hardwarová bezpečnost

# Trustworthy solution

## HW Anchored Secure Boot

Image Signing and Secure Boot work together to ensure that authentic Cisco SW boots up on a Cisco Platform

## Secure Unique Device Identification

Tamperproof ID for the device

## Trust Anchor Module

HW Authenticity Check

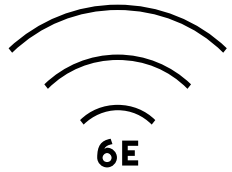


Přístup do sítě

# WLAN has inherent vulnerabilities, exposing it to various threats



# Industry's best and broadest Wi-Fi 6E and Wi-Fi 6 portfolio



# Securing AP Switch Port Access



802.1x  
Authentication  
(EAP-FAST, EAP-  
PEAP, or EAP-TLS)



How do we bootstrap configure the AP?

The screenshot shows the 'Add AP Join Profile' configuration window in a network management system. The 'Management' tab is selected, and the 'Credentials' section is active. The 'Dot1x Credentials' section contains the following fields:

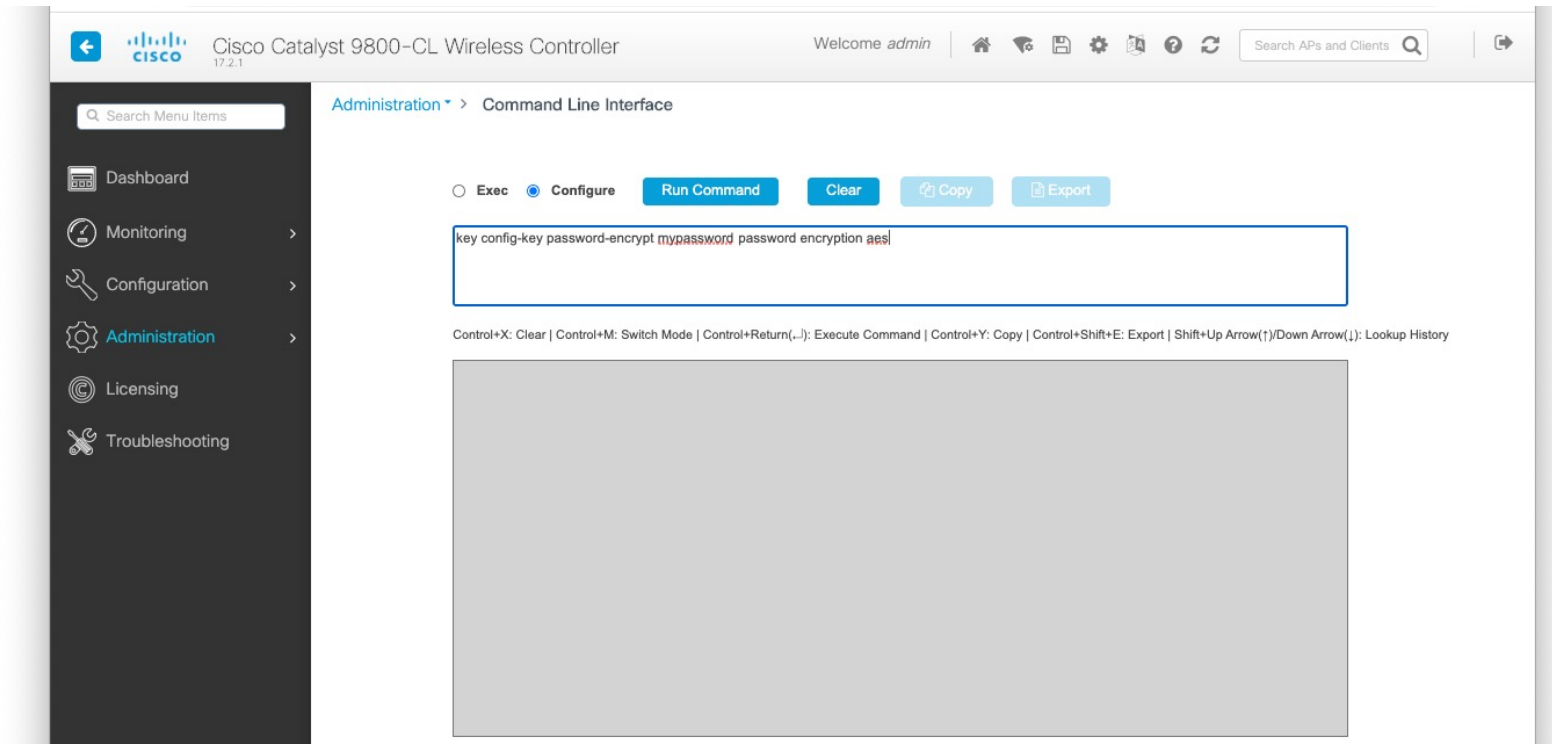
Field	Value
Dot1x Username	Enter dot1x Username
Dot1x Password	Enter Dot1x Password
Dot1x Password Type	clear

At the bottom of the window, there are 'Cancel' and 'Apply to Device' buttons.



# Encrypt keys and passwords

```
key config-key password-encrypt mypassword  
password encryption aes
```



The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller web interface. The top navigation bar includes the Cisco logo, the device name "Cisco Catalyst 9800-CL Wireless Controller", the version "17.2.1", and a "Welcome admin" message. A search bar for "Search APs and Clients" is also present. The left sidebar contains a "Search Menu Items" field and a list of navigation options: Dashboard, Monitoring, Configuration, Administration (highlighted), Licensing, and Troubleshooting. The main content area is titled "Administration > Command Line Interface". It features two radio buttons: "Exec" (unselected) and "Configure" (selected). Below these are buttons for "Run Command", "Clear", "Copy", and "Export". A text input field contains the command: "key config-key password-encrypt mypassword password encryption aes". Below the input field, a legend of keyboard shortcuts is provided: "Control+X: Clear | Control+M: Switch Mode | Control+Return(...): Execute Command | Control+Y: Copy | Control+Shift+E: Export | Shift+Up Arrow(↑)/Down Arrow(↓): Lookup History". A large grey rectangular area is visible below the legend, likely representing the output of the command.

Ověření klienta?



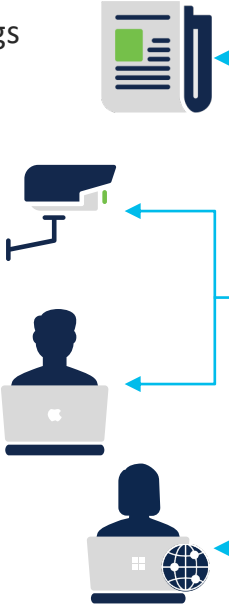
# Zero Trust for the Workplace

## Enterprise

---

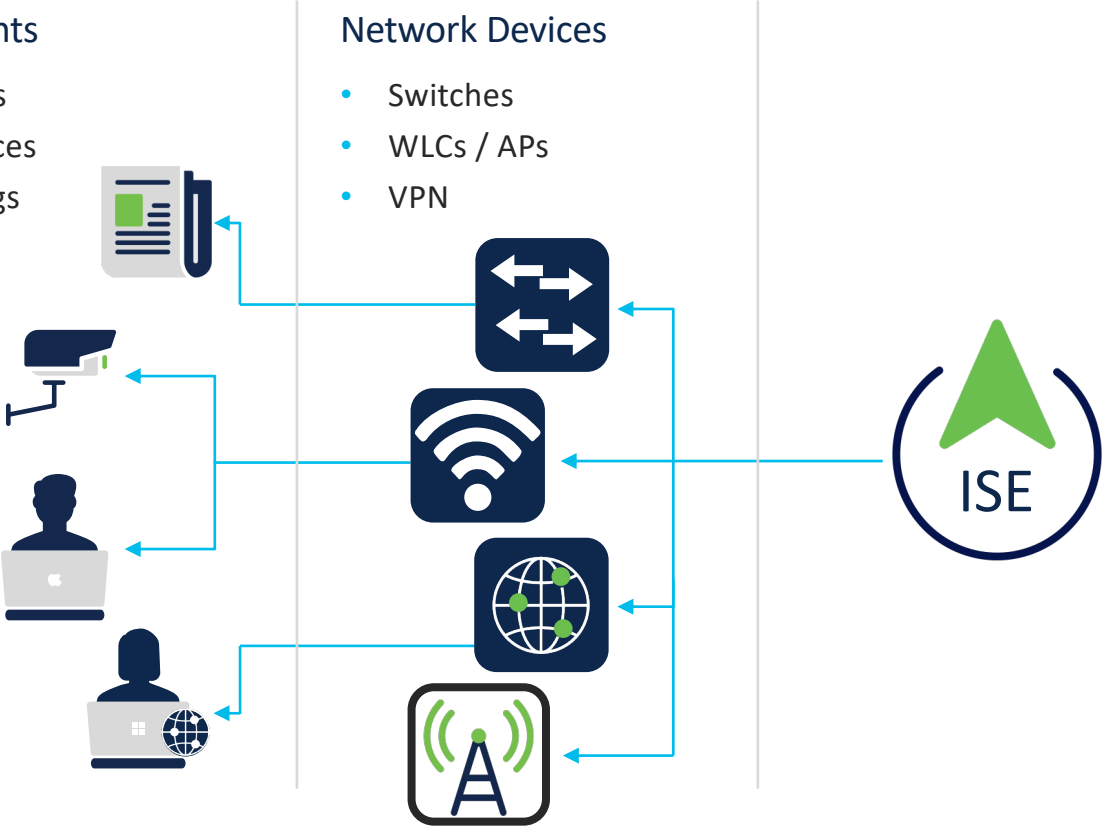
### Endpoints

- Users
- Devices
- Things



### Network Devices

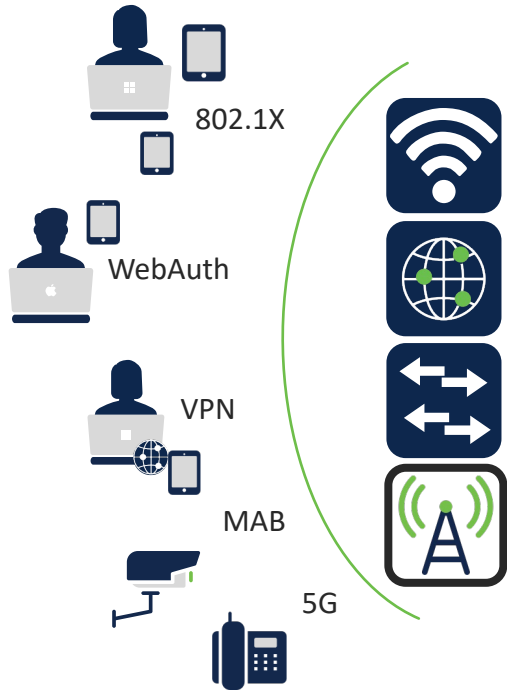
- Switches
- WLCs / APs
- VPN



# ISE Secure Access Control Options

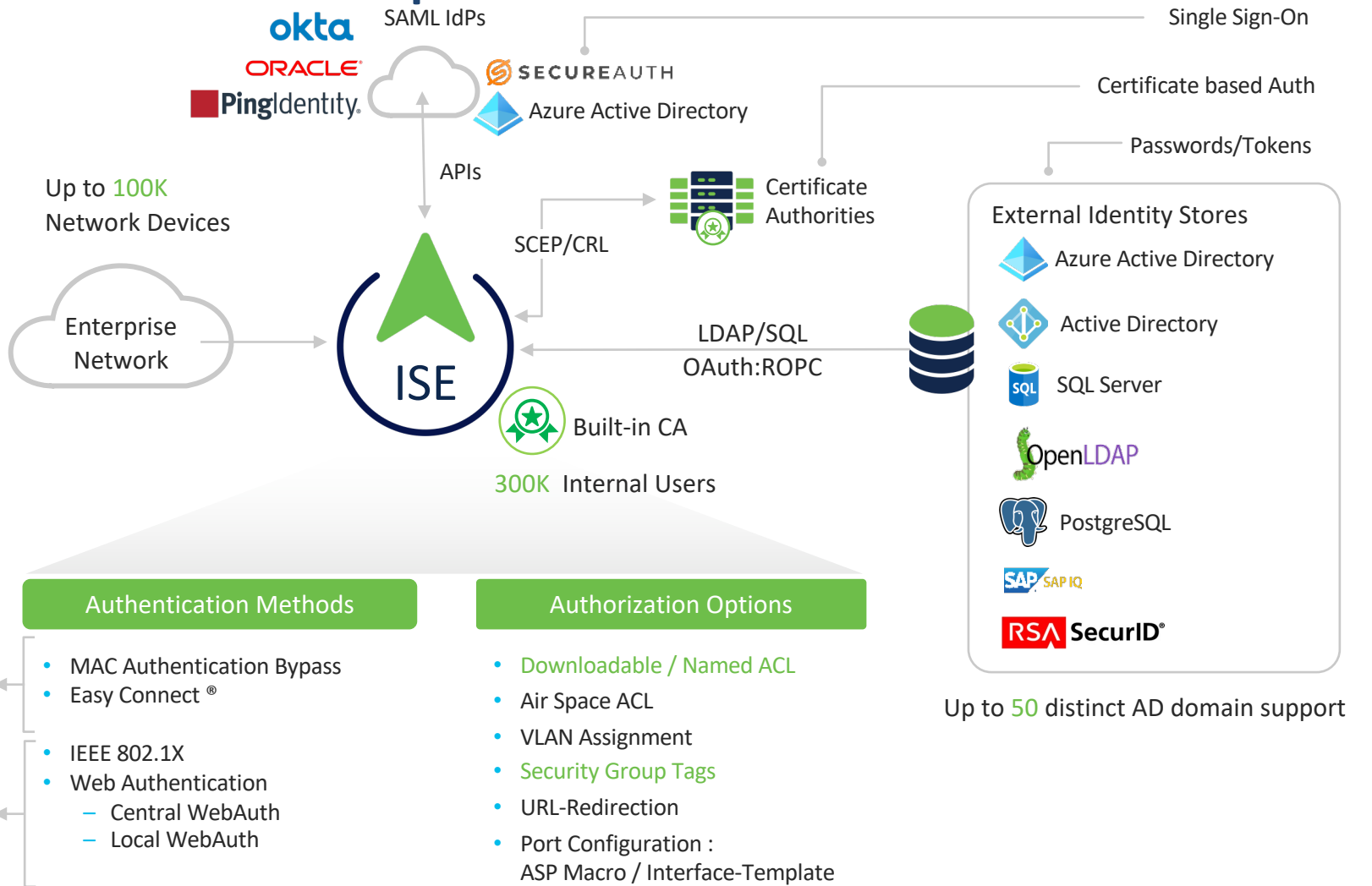
Native Supplicants | Cisco Secure Client

2,000,000 concurrent sessions



Passive Identity

Active Identity



# What can be done with RCM

- In Enterprise networks, you may need to know how many devices are using RCMs

Device Name	MAC Address	IPv4 Address	Device Type	Health	Usage	AP Name	Band	RSSI	SGT	Location
Device123		37	Complex-Device	5	1.25 GB	C9120.C178	5 GHz	-19 dBm	Tag Name	San Jose/SJC04
Device124		35	Complex-Device	5	1.25 GB	C9120.C179	5 GHz	-21 dBm	Tag Name	San Jose/SJC04
Device125		23	Complex-Device	10	1.25 GB	C9120.C180	5 GHz	-42 dBm	Tag Name	San Jose/SJC04
Device126		12	Complex-Device	10	1.25 GB	C9120.C181	5 GHz	-20 dBm	Tag Name	San Jose/SJC04
Device127		65	Complex-Device	8	1.25 GB	C9120.C182	5 GHz	-17 dBm	Tag Name	San Jose/SJC04
Device128	CE:DE:31:BC:BE:D9	10.10.103.98	Complex-Device	3	1.25 GB	C9120.C183	5 GHz	-19 dBm	Tag Name	San Jose/SJC04
Device129	B4:E4:31:BC:BE:D7	10.10.103.23	Complex-Device	9	1.25 GB	C9120.C184	5 GHz	-21 dBm	Tag Name	San Jose/SJC04
Device130	09:67:31:BC:BE:D7	10.10.103.22	Complex-Device	10	1.25 GB	C9120.C185	5 GHz	-42 dBm	Tag Name	San Jose/SJC04
Device131	AT:DE:31:BC:BE:D7	10.10.103.11	Complex-Device	10	1.25 GB	C9120.C186	5 GHz	-20 dBm	Tag Name	San Jose/SJC04
Device132	GG:DE:31:BC:BE:D7	10.10.103.09	Complex-Device	8	1.25 GB	C9120.C187	5 GHz	-17 dBm	Tag Name	San Jose/SJC04

- In MDM-based networks, you may need to prevent users from mistakenly activating RCM on enterprise assets

Configuration - Edit WLAN

General Security **Advanced** Add To Policy Tags

Coverage Hole Detection  Universal Admin

Aironet IE  OKC

Advertise AP Name  Load Balance

P2P Blocking Action Disabled Band Select

Multicast Buffer  DISABLED IP Source Guard

Media Stream Multicast-direct  WMM Policy Allowed

11ac MU-MIMO  mDNS Mode Bridging

WiFi to Cellular Steering

Fastlane+ (ASR)

Deny LAA clients

Max Client Connections

Per WLAN 0

Per AP Per WLAN 0

Per AP Per AP Per WLAN 0

Off Channel Scanning Defer

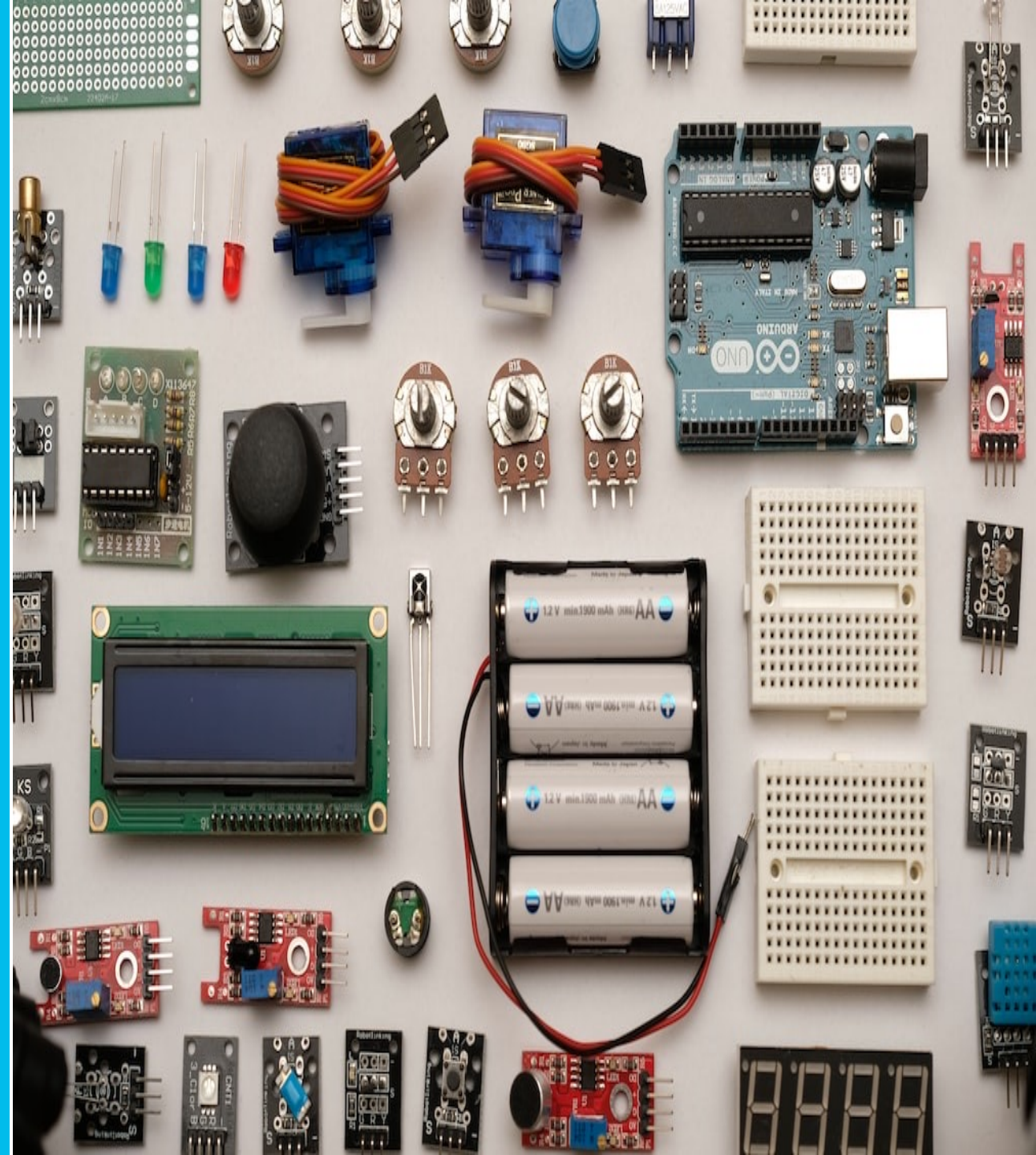
Defer Priority  0  1  2  3  4  5  6  7

Scan Defer Time 100

Assisted Roaming (11k)

Update & Apply to Device

# IoT



# Multi-Preshared Key

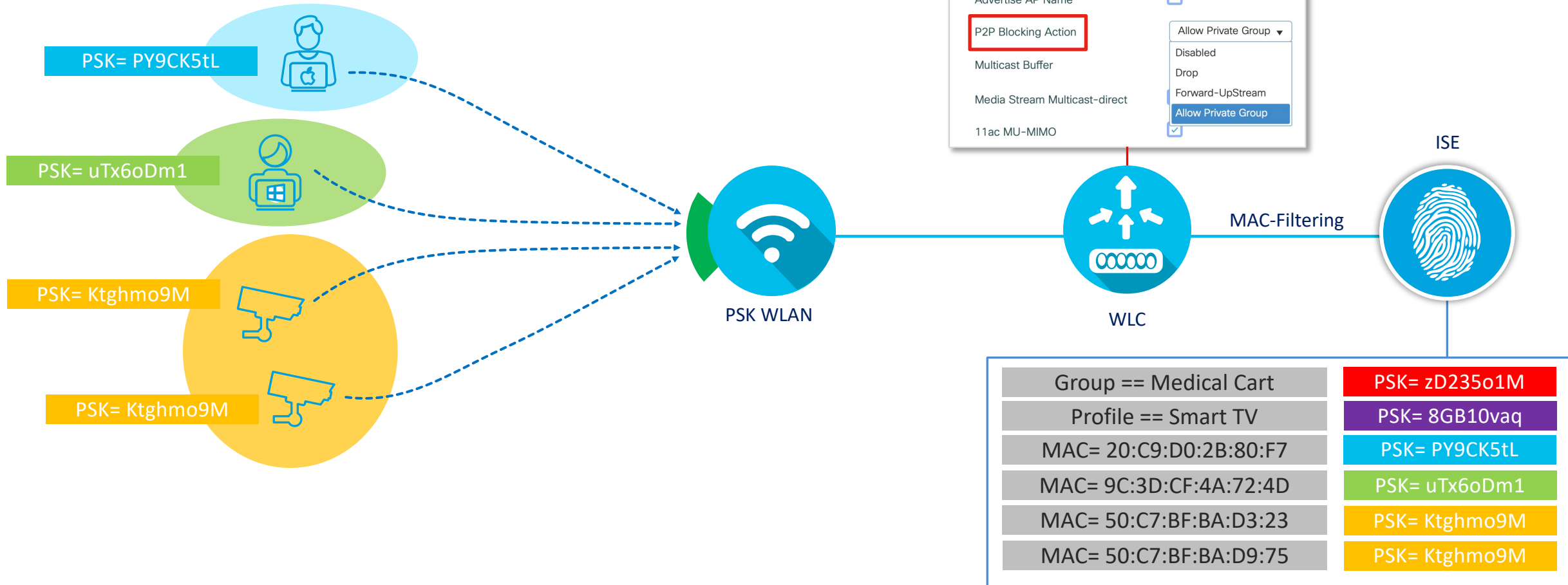
- Multi-Preshared Key (MPSK) supports multiple PSKs simultaneously on a single SSID
- Any of the configured PSKs can be used to join the network
- This is different from the Identity PSK (iPSK), where unique PSKs are created for individuals or groups of users on the same SSID

The screenshot shows the 'Edit WLAN' configuration interface. At the top, the security mode is set to 'WPA + WPA2'. Below this, there are checkboxes for 'MAC Filtering' and 'Lobby Admin Access', both of which are currently unchecked. The 'WPA Parameters' section includes 'WPA Policy' (unchecked), 'WPA2 Policy' (checked), 'GTK Randomize' (unchecked), and 'OSEN Policy' (unchecked). The 'WPA2 Encryption' section shows 'AES(CCMP128)' (checked) and 'GCMP128' (unchecked). The 'Protected Management Frame' section has 'PMF' set to 'Disabled'. The 'Fast Transition' section shows 'Status' as 'Adaptive Enabled', 'Over the DS' (unchecked), and 'Reassociation Timeout' set to '20'. The 'Auth Key Mgmt' section includes '802.1x' (unchecked), 'Easy-PSK' (unchecked), 'FT + 802.1x' (unchecked), '802.1x-SHA256' (unchecked), 'PSK' (checked), 'CCKM' (unchecked), 'FT + PSK' (unchecked), and 'PSK-SHA256' (unchecked). The 'PSK Format' is set to 'ASCII' and 'PSK Type' is 'Unencrypted'. A 'Pre-Shared Key\*' field contains a masked password. The 'MPSK Configuration' section has 'Enable MPSK' checked. Below this are '+ Add' and 'Delete' buttons. A table lists the configured PSKs:

Priority	Key Format	Password Type
<input type="checkbox"/> 0	ASCII	Unencrypted
<input type="checkbox"/> 1	ASCII	Unencrypted

At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons. A modal window is open in the foreground with the following fields: 'Priority \*' (2), 'Key Format' (ASCII), 'Password Type' (Unencrypted), and 'Pre-Shared Key\*' (masked). It has 'Cancel' and 'Apply' buttons.

# Identity Preshared Key





# 6GHz WLAN Design Considerations

## 6GHz SSID Requirements

- WPA3 L2 Security: OWE, SAE or 802.1x-SHA256
- Protected Management Frame (PMF) enabled
- Any non-WPA3 L2 security method is not allowed – **no mixed mode possible**

## What options would you have?

1. “ALL-IN” option: Reconfigure the existing WLAN to WPA3, one SSID for all radio policies (2.4/5/6 GHz) – **Most unlikely**
2. “One SSID” option: Configure multiple WLANs with the same SSID name, different security settings – **Most conservative**
3. “Multiple SSIDs” option: Redesign your SSIDs, adding specific SSID/WLAN with specific security settings – **Most flexible**

Most likely your current SSID configuration would prevent it from being broadcasted on 6GHz

Note: as 17.9.1, there is a limit of 8 SSIDs broadcasted on 6GHz radio

AKM = Authentication and Key Management  
OWE = Opportunistic Wireless Encryption  
SAE = Simultaneous Authentication of Equals  
SHA-256 = Secure Hash Algorithm (SHA) 256 bit

Návštěvnická Wi-Fi



#nePINdej!

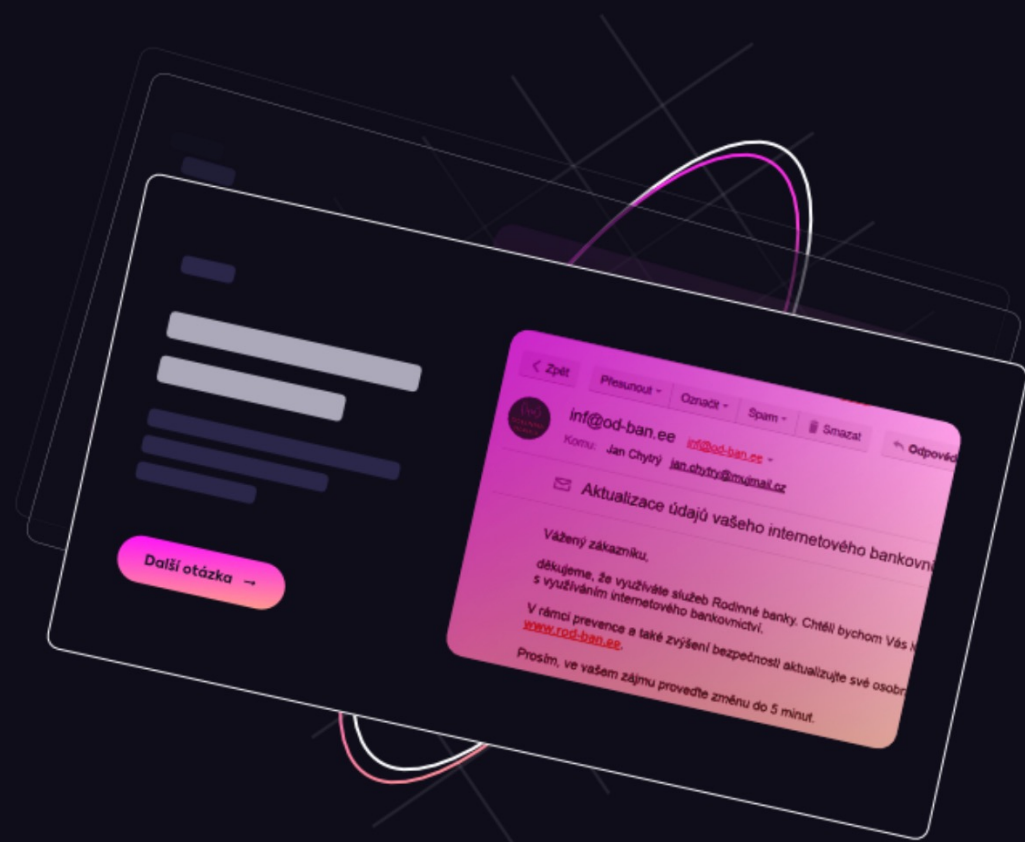
# Bud'te na internetu v bezpečí

Odhalíte včas, že na vás útočí online podvodníci? Vyzkoušejte si náš nový **interaktivní test** a zjistěte, jak jste na tom. Vítězí ten, kdo nePINdá!

#nePINdej!

Spustit test →

O projektu



## Otázka č. 1

Než začneme s naším testem, je potřeba se připojit na Wi-Fi. Dostupné máte tři veřejné sítě. Rozhodněte se, na kterou z nich je nejbezpečnější se připojit. Na jednotlivé sítě můžete kliknout. Připojením na špatnou síť můžete přijít až o 5 000 Kč. Vyberte, ke které síti se připojíte.

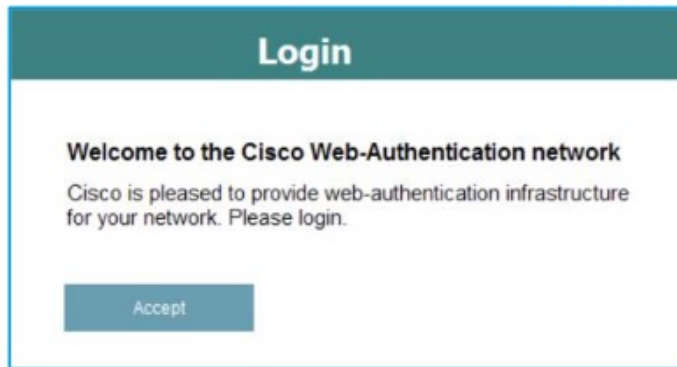


Portály



# In few words

WLC



The screenshot shows a login page with a teal header containing the word "Login". Below the header, there is a section titled "Welcome to the Cisco Web-Authentication network" with a sub-header "Cisco is pleased to provide web-authentication infrastructure for your network. Please login." At the bottom of the page is a teal button labeled "Accept".

- Native and easy to use.
- Ideal for passthrough with AUP pages.
- LWA with consent.

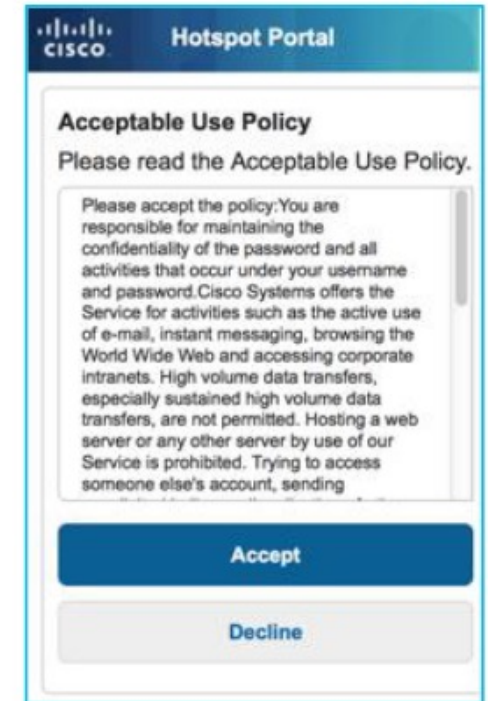
Cisco DNA Spaces



The screenshot shows a login page for "Cisco Live!". It features the "Cisco Live!" logo at the top, followed by a background image of a stadium filled with people. Below the image, there is a welcome message: "Welcome to Cisco Live Guest Wi-Fi. Please fill in the form below to connect." The form contains three input fields: "Your Name Here\*", "Your Company Name Here\*", and "Your Country Here\*", each with a clear button (X). At the bottom is a blue button labeled "CONNECT".

- Very easy/powerful to customize and assign portals based on sites.
- Ideal for passthrough with AUP pages, or for one-time SMS/email codes.
- LWA with consent.

ISE

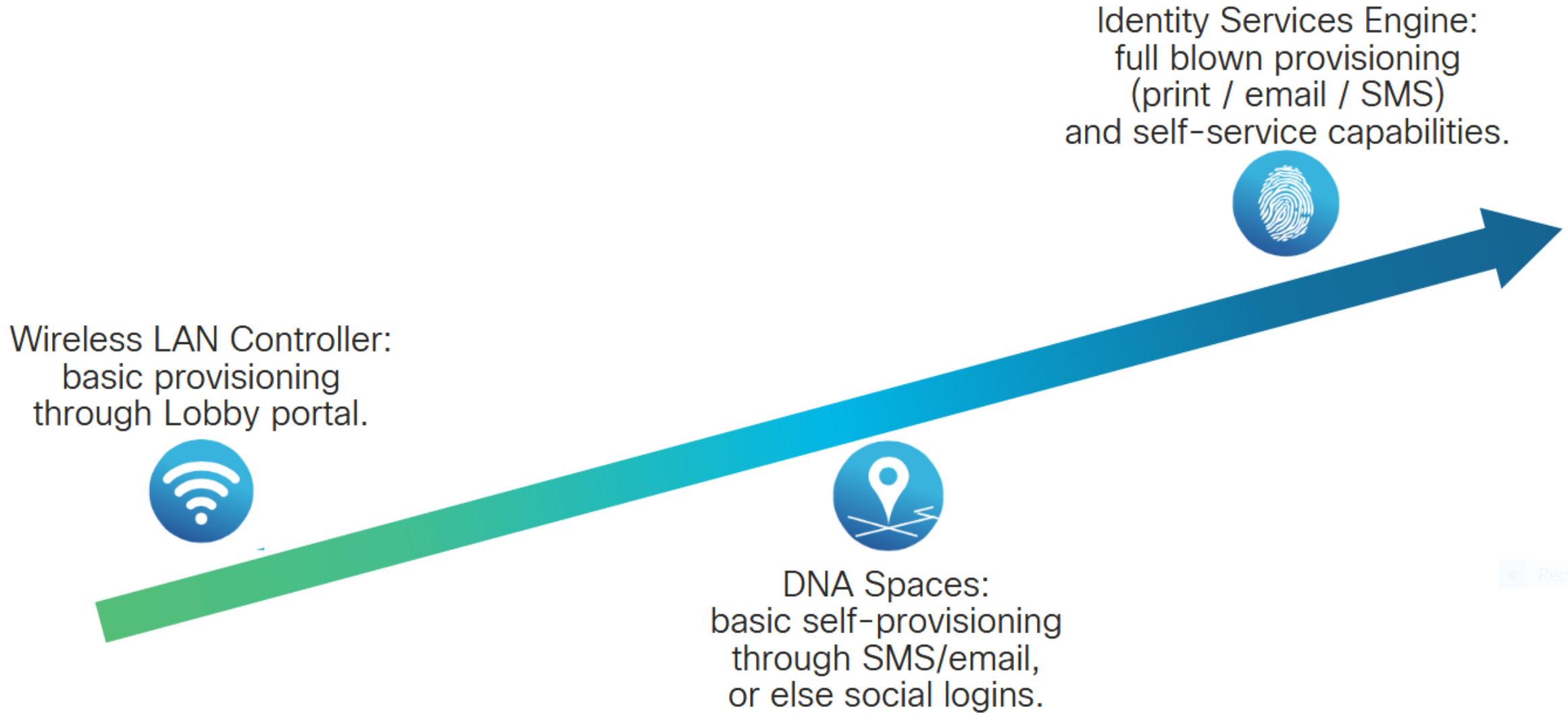
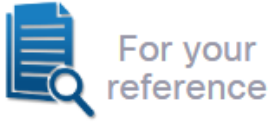


The screenshot shows a "Hotspot Portal" with the Cisco logo in the top left. The main heading is "Acceptable Use Policy" with the instruction "Please read the Acceptable Use Policy." Below this is a scrollable text area containing the policy details. At the bottom of the page are two buttons: a blue "Accept" button and a grey "Decline" button.

- Most versatile solution.
- Ideal both for login and AUP portals.
- It requires an additional learning curve.
- LWA or CWA.

*used live!*

# Guest provisioning choices



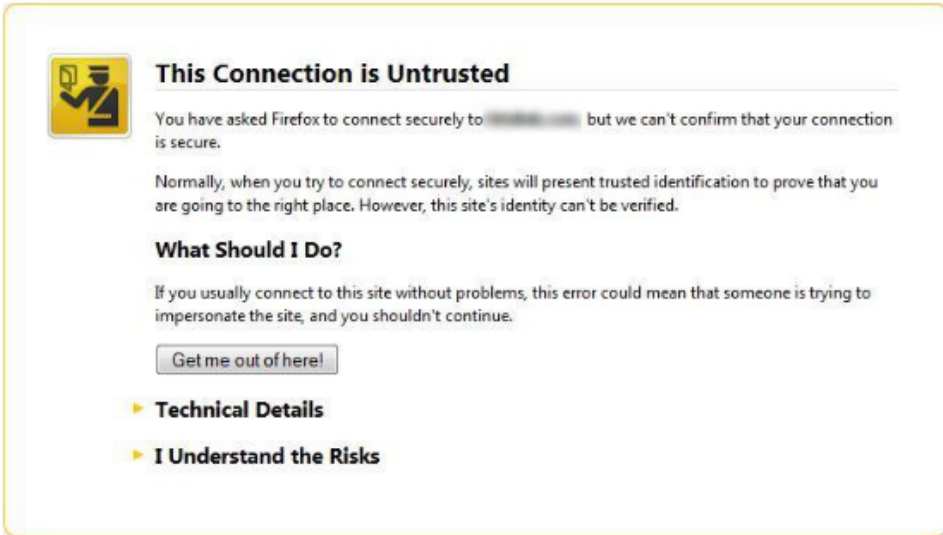
LWA





# LWA and certificates

## WLC's internal portal



**This Connection is Untrusted**

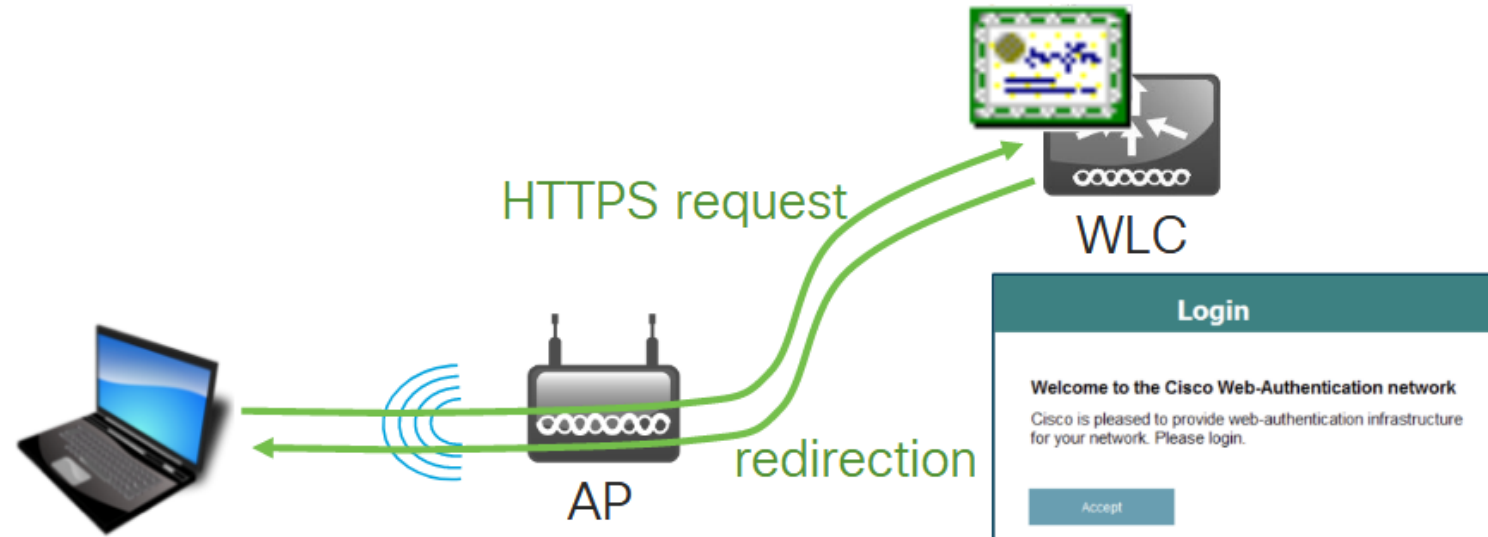
You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

- ▶ **Technical Details**
- ▶ **I Understand the Risks**



Certificates for the Controller Web Authentication:


<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html>

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#anc20>

CWA



# CWA and certificates



### This Connection is Untrusted

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

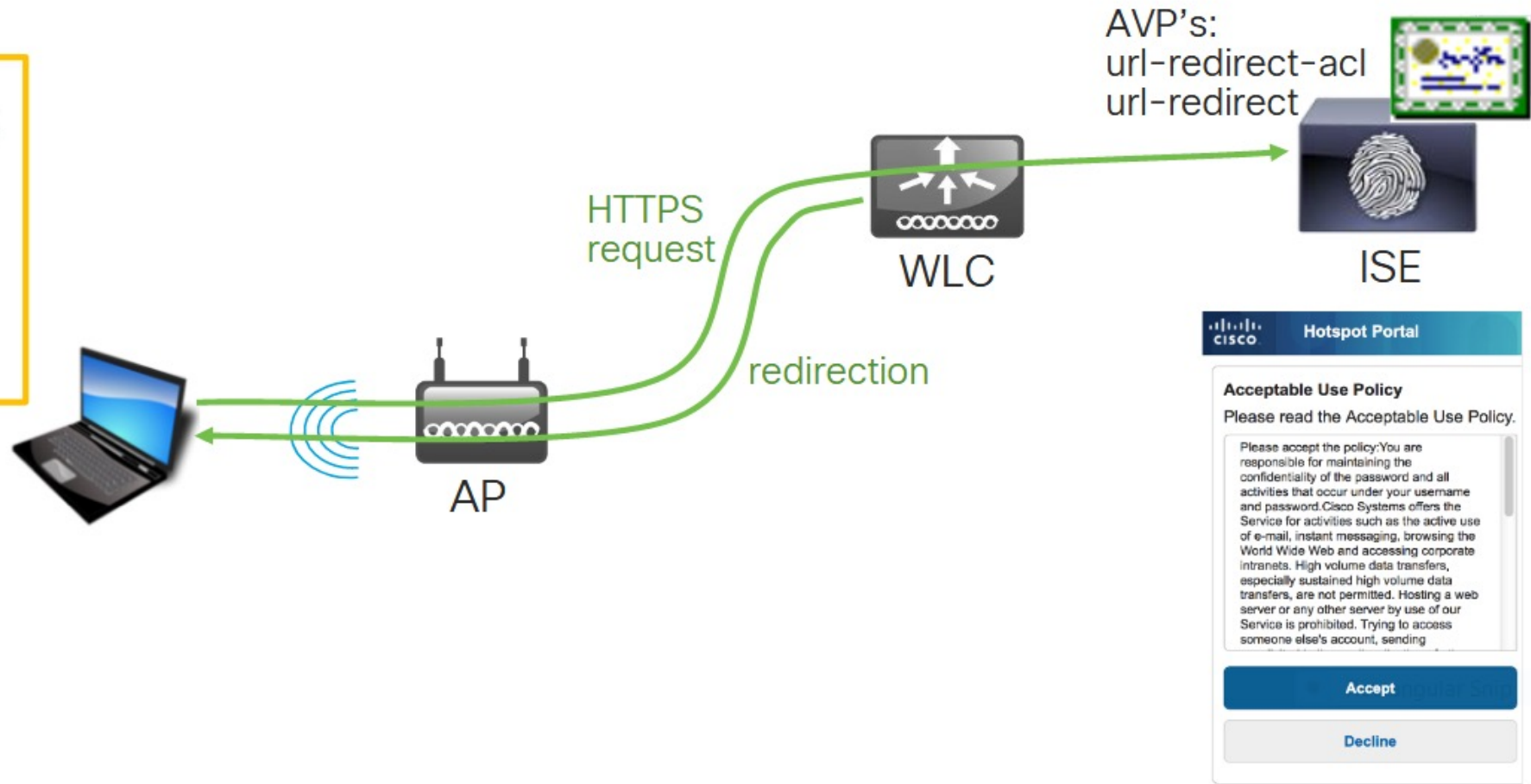
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.


#### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- Technical Details
- I Understand the Risks





### Hotspot Portal

#### Acceptable Use Policy

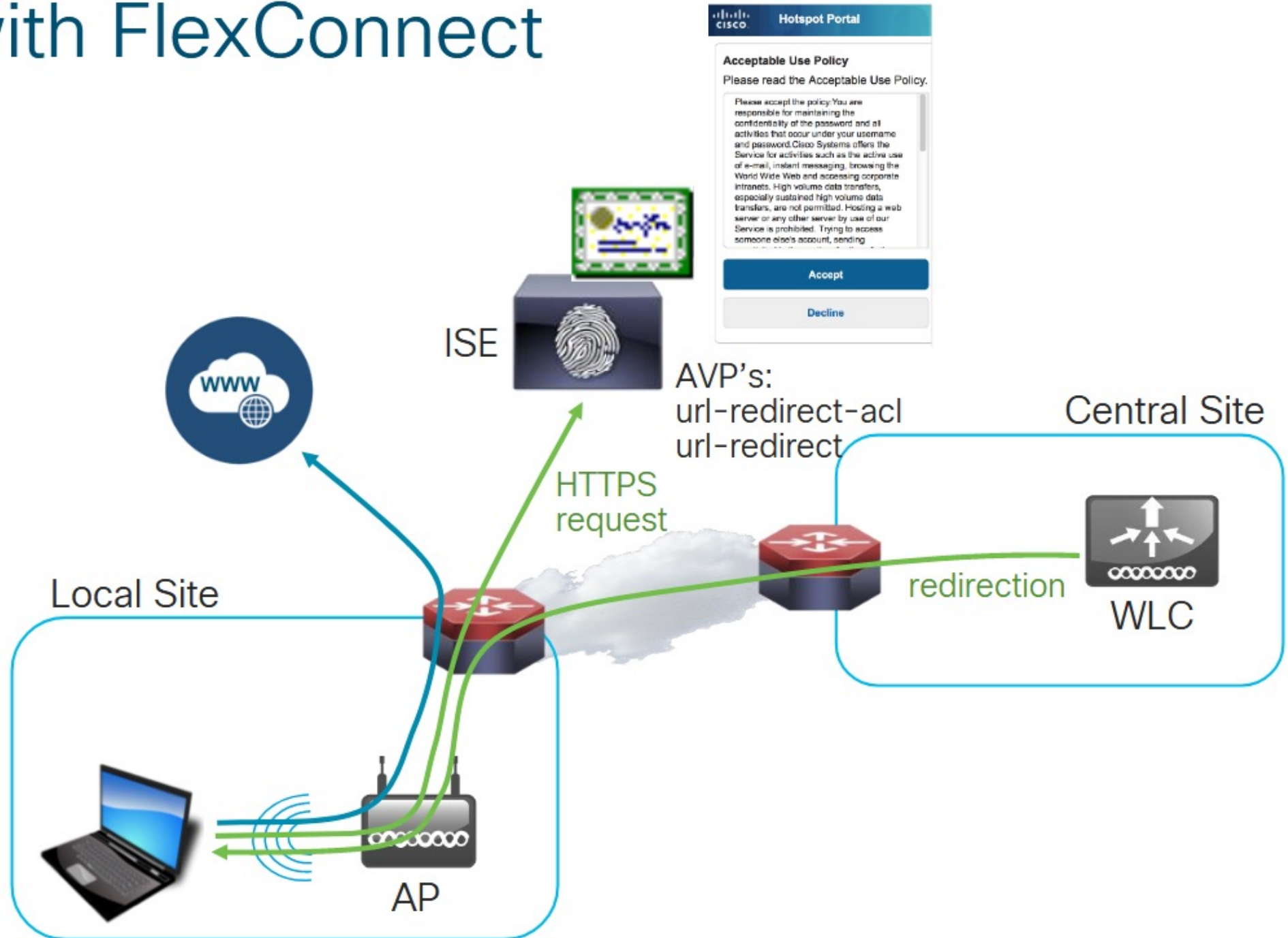
Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

[Accept](#)

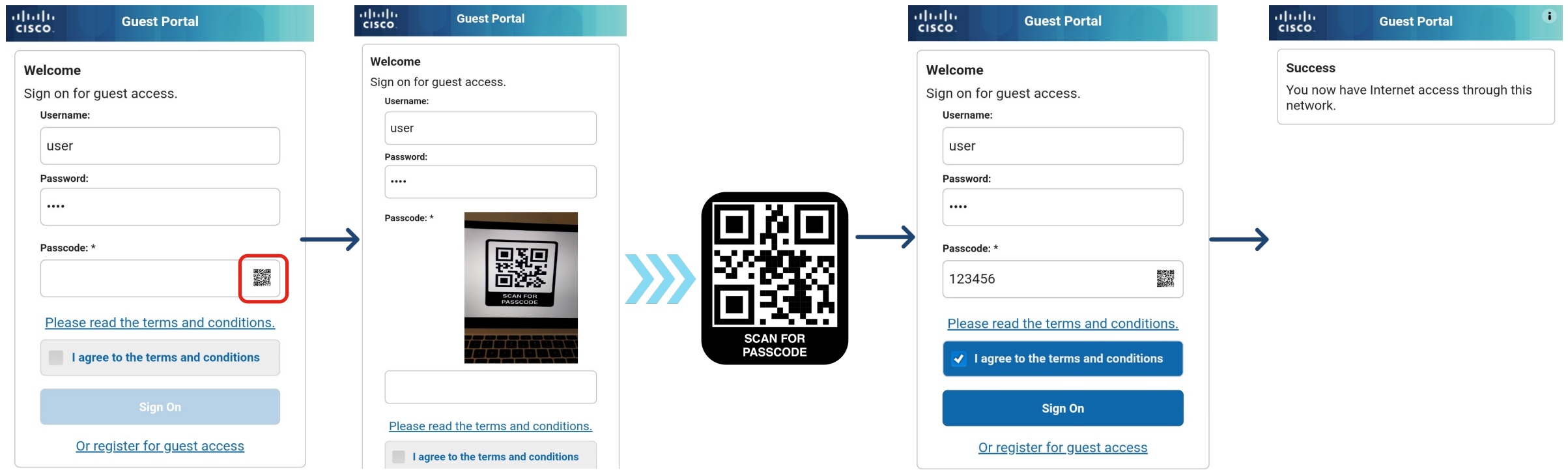
[Decline](#)

# CWA with FlexConnect



# QR Code Scanning in ISE Guest Portal

- (1) Guest fills persona fields
- (2) Guest presses QR code button
- (3) Passcode is autofilled
- (4) Access is granted



*Další možnosti pro veřejné sítě*

OWE



# Wi-Fi Certified Enhanced Open

The next generation of hotspot security

- Another WFA certification, not part of WPA3, mostly for hotspots.
- Based on Opportunistic Wireless Encryption (OWE): APs and clients will be able to automatically negotiate encryption.
- It prevents passive attacks (i.e., traffic visibility).



Endpoints not supporting Enhanced Open might not correctly see/connect to an SSID with Enhanced Open configured.  
But...

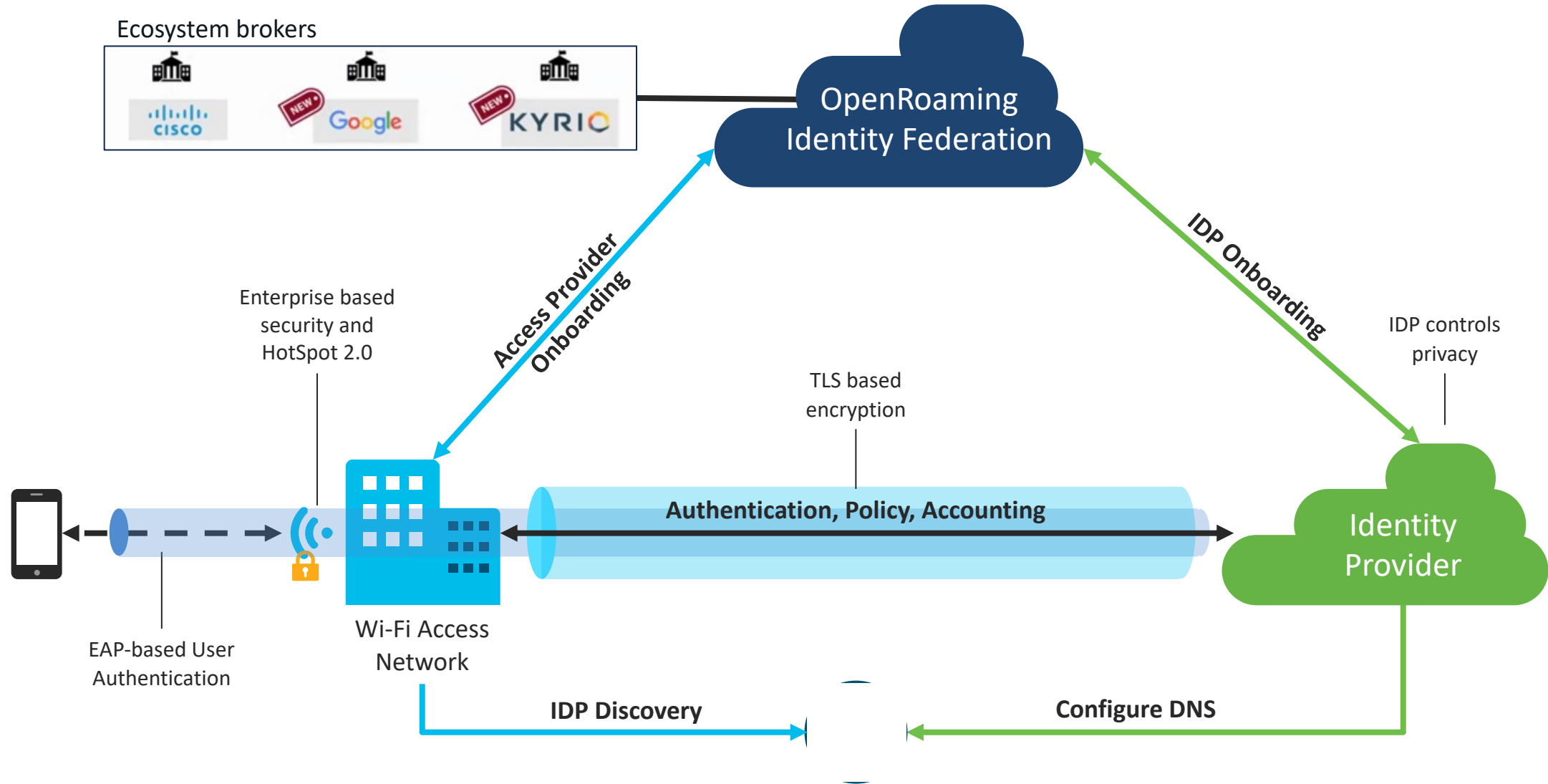




# OpenRoaming



# Secure Wi-Fi Onboarding



# OpenRoaming Identity Principles

1

## Authentication is private

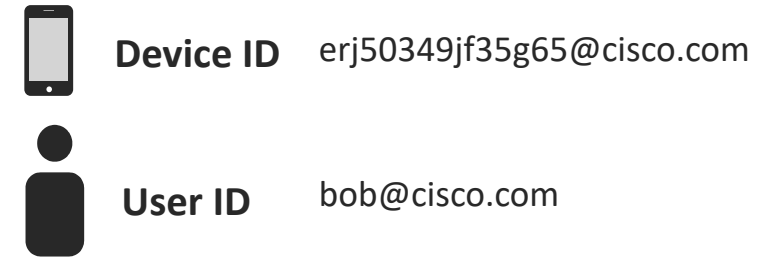
Secure and private authentication between user's device and IDP



2

## User and device are identified in context

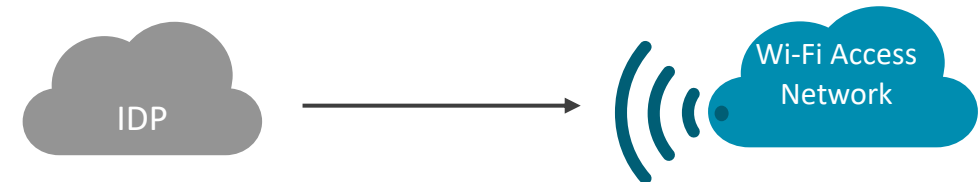
Identified with persistent Device ID and User ID with IDP context  
IDP shares (anonymized) data in the secured path



3

## IDP shares identities on the user's behalf

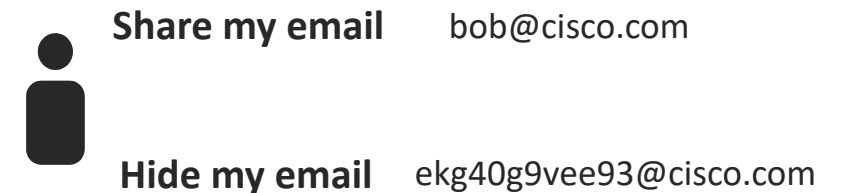
IDP manages identity and privacy for the user



4

## Privacy with user consent

User controls privacy, identifiers are always persistent



# Next Gen Onboarding Client Matrix

## OpenRoaming App Compatibility

Native OS Support	OR Mobile App
Samsung Devices: Android 10 or higher Google Pixel: Android 11 or higher	Apple devices running iOS 13.3 or higher Android phones running Android 9 or higher

## DNA Spaces SDK Compatibility

Apple iOS	Android
iOS 13.3 or higher XCode version 12 or higher	Android 9 or higher

# *Secure Network Analytics*

# Secure Network Analytics

## Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

## Global threat intelligence (powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation

TALOS

## Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

A box containing a 4x3 grid of binary code (0s and 1s) in green, a green line graph with a magnifying glass over a bar chart, and three red warning triangles at the bottom.

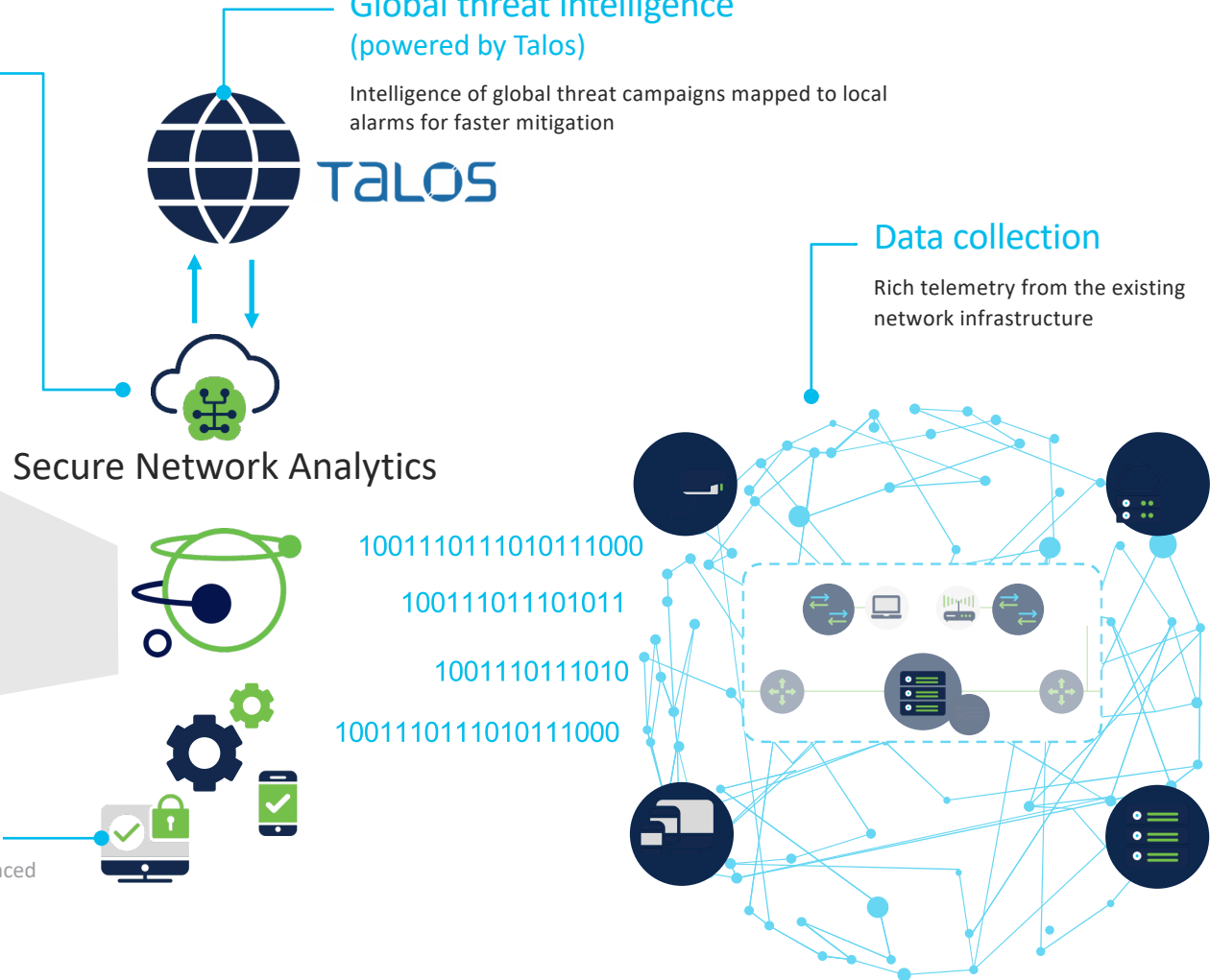
## Secure Network Analytics

## Data collection

Rich telemetry from the existing network infrastructure

## Encrypted traffic analytics

Malware detection without any decryption using enhanced telemetry from the Cisco devices



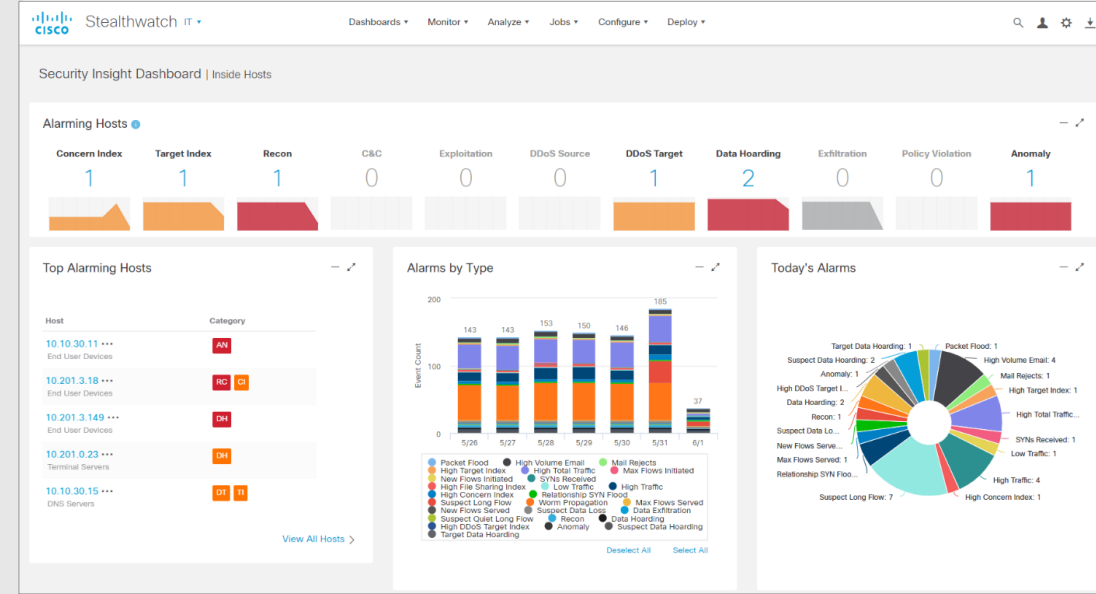
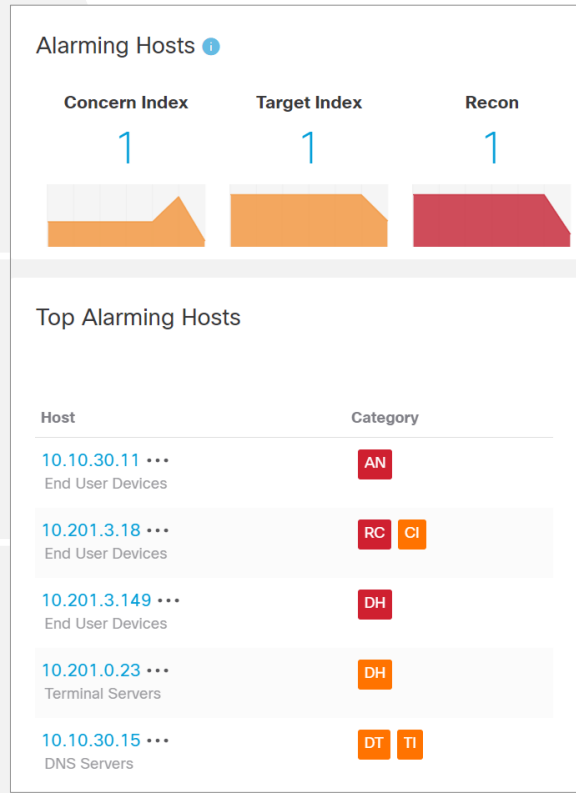
1001110111010111000  
100111011101011  
1001110111010  
1001110111010111000

# Detected Alarms tied to entities

Quick snapshot of malicious activity

Suspicious behavior linked to logical alarms

Risks prioritized to take immediate action



Relevant use cases:  
Detecting Top Alarming Hosts on the network

# Comprehensive host investigation

## Host summary



10.201.3.18

Flows

History

*Hostname:* dhcp-atl-4-71.acme.com

*Host group:* Desktops, Sales

*Location:* Atlanta, GA

*First Seen:* 1/25/20 1:52 AM

*Last Seen:* 6/1/21 8:31 AM

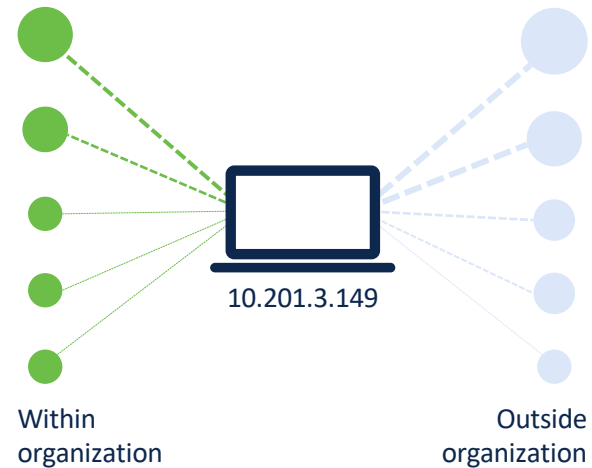
*Policies:* Insider Threat Event,  
Client IP Policy

Quarantine

Unquarantine

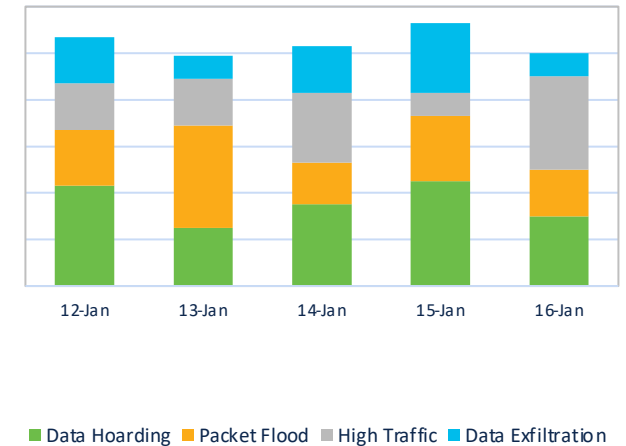
Summary of aggregated  
host information

## Traffic by peer host group



Observed  
communication patterns

## Alarms by Type



Historical  
alarming behavior



# Granular host event investigation

Determine if a host is a source or destination of events

Top Security Events for 10.201.3.149

Source (10) Target (1)

Security Event	Count	Concern Index	First Active	Target Host	Target Host Group	Actions
▶ Suspect Data Hoarding	1	515,341	06/01 2:45:00 AM	Multiple Hosts	--	...
▼ Suspect Data Loss	2	28,493	06/01 6:25:00 AM	Multiple Hosts	--	...
<b>DETAILS</b>		<b>DESCRIPTION</b>				
Observed 24.41M bytes. Expected 0 bytes, tolerance of 0 allows up to 10M bytes.		Suspect Data Loss: Indicates that an inside host has uploaded an abnormal amount of data to outside hosts.				
▶ Packet Flood - 22	1	5,600	06/01 2:41:33 AM	10.201.0.72 ...	Atlanta , Compli	...
▶ Flow_Denied - 443	14	2,268	06/01 2:08:59 AM	98.129.93.174 ...	United States	...
▶ Flow_Denied - 80	11	1,782	06/01 2:10:19 AM	64.14.29.85 ...	United States	...
▶ Flow_Denied - 443	6	972	06/01 2:11:23 AM	204.93.223.146 ...	United States	...

Associated Flows Edit

Top Reports >

External Lookup >

---

Subject IP: 10.10.0.20

Peer IP: 10.20.0.30

from: 09/06 8:00 AM

to: 09/06 2:24 PM

Security event details to understand why the alarm was triggered and see the policies and threshold values that were violated

Use actions to drill down into the telemetry associated with the security event with just one click



Relevant use cases:  
Using the Security Event Workflow

# Investigating Telemetry via flow search

Flow Search ⓘ Load Saved Search Save Search

Clear All Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: Either (Orientation)

Connection: All (Flow Direction)

SEARCH TYPE: Flow

TIME RANGE: Last 5 minutes

SEARCH NAME: Flow on 9/6/2017 at 12:05 PM

MAX RECORDS RETURNED: 2,000

**Subject**

HOST IP ADDRESS:

HOST GROUPS: Select

▶ Advanced Subject Options ⓘ

**Connection**

PORT / PROTOCOL:

APPLICATIONS: Select

▶ Advanced Connection Options ⓘ

**Peer**

HOST IP ADDRESS:

HOST GROUPS: Select

▶ Advanced Peer Options ⓘ

Set the maximum number of records returned

MAX RECORDS RETURNED

- 2,000
- 1,000
- 2,000**
- 10,000
- 20,000 - Download CSV File Only
- 50,000 - Download CSV File Only
- 100,000 - Download CSV File Only

Common search parameters available through Basic search



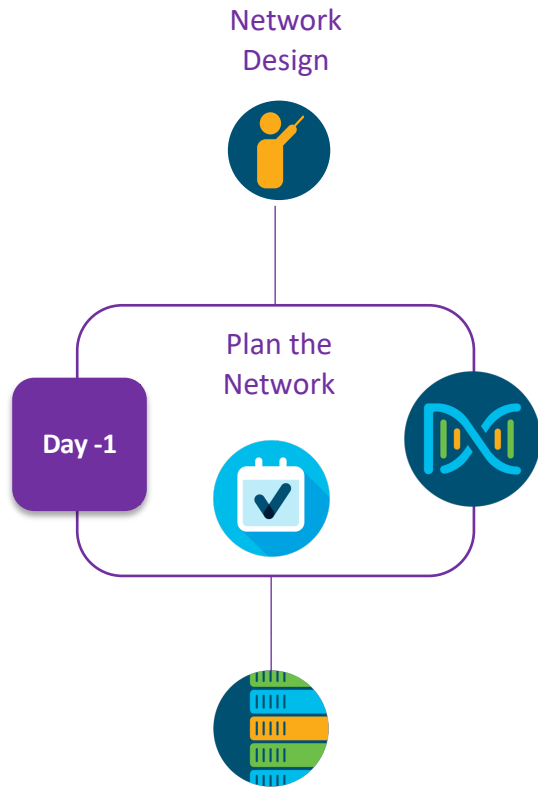
Relevant use cases:

- Monitoring Trusted Third Party
- Monitoring Vendor Activity
- Investigating Unidirectional Traffic
- Obtaining Historical Conversations for Unauthorized Data Transfer

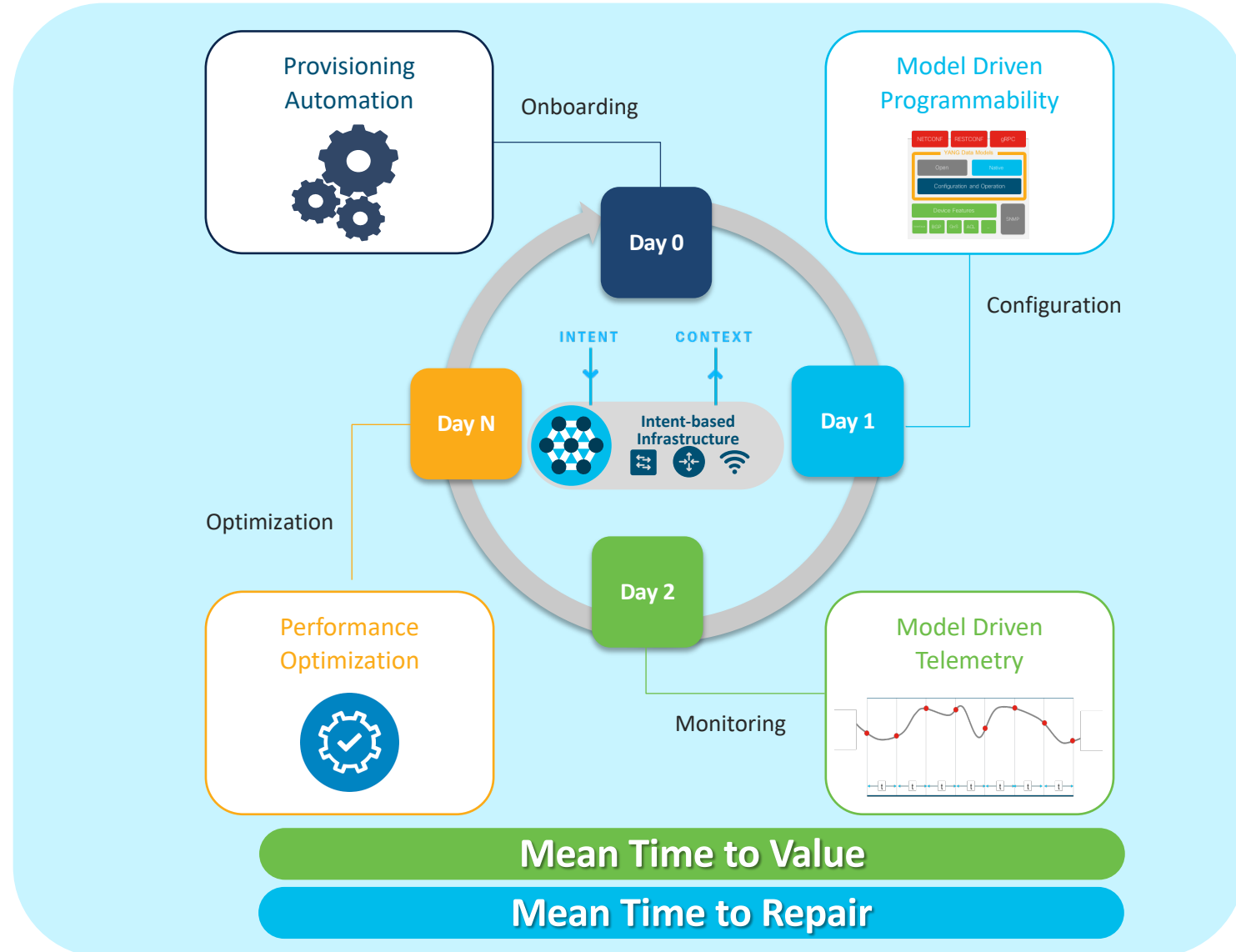
DNA Center a Spaces

# Cisco DNA Automation and Assurance

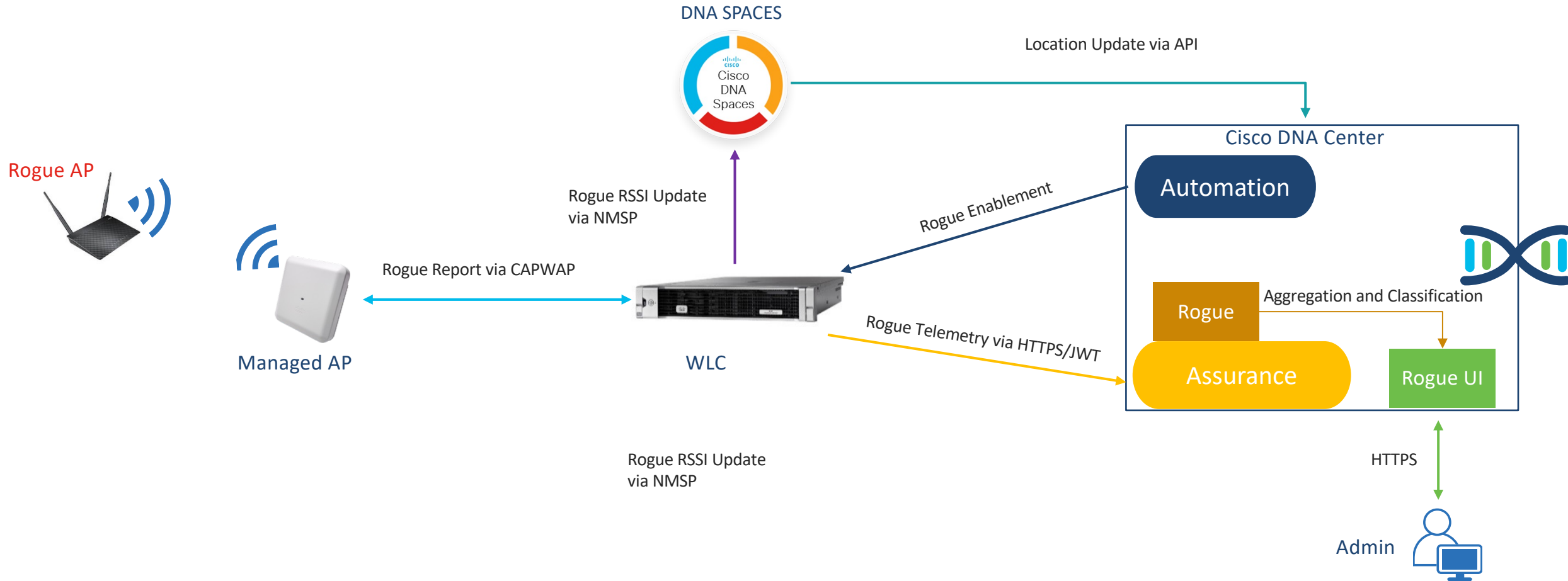
Automation across an Intent-Based Lifecycle



- servicenow ITSM
- Infoblox IPAM
- ekahau Design



# Rogue Management Architecture



# Rogue Management and aWIPS on Wi-Fi 6E

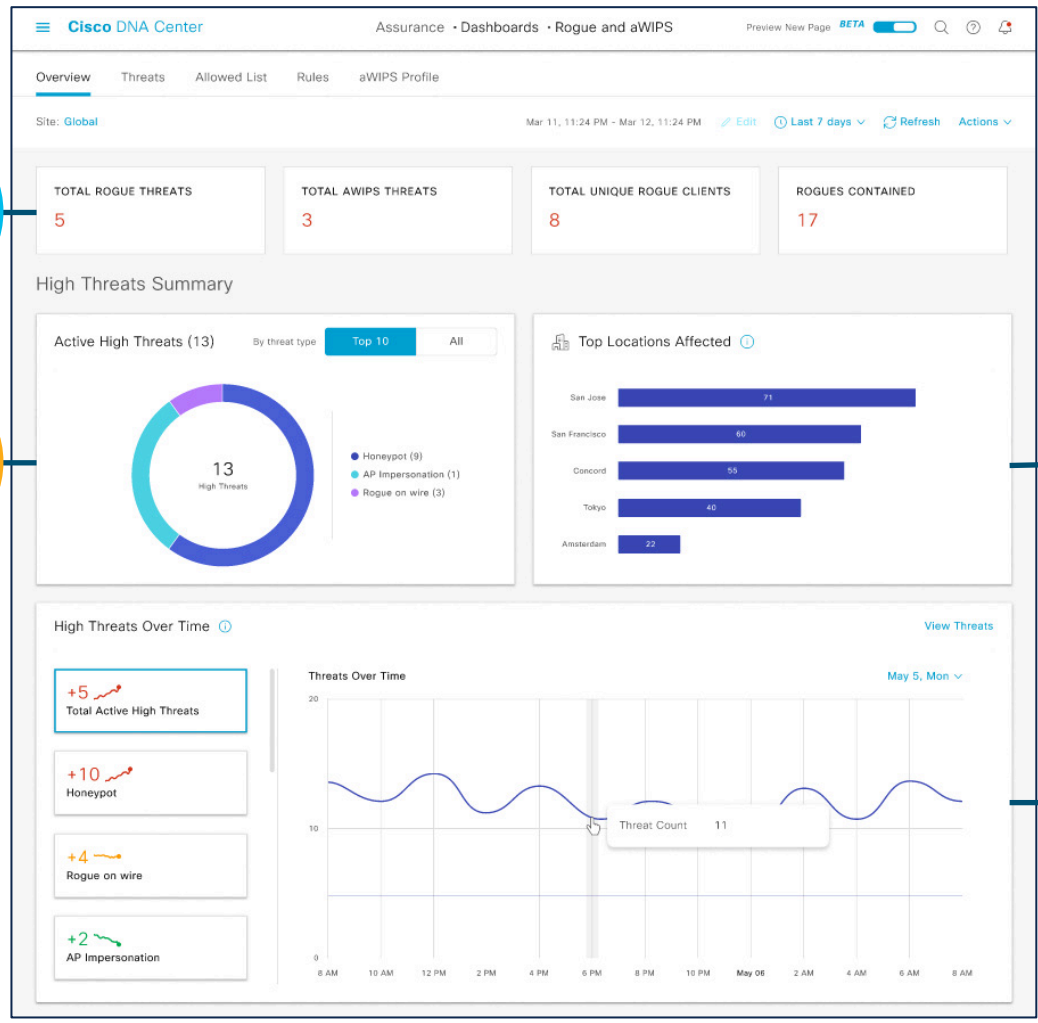
## Abolish your 6 GHz Network Vulnerabilities from 2.3.2

Threat Insights

High Threats by Category

Top Locations Affected

High Threats Over Time



Note: Revamped UI is from 2.3.4

# Forensic Captures

Cisco DNA Center Assurance · Dashboards · Rogue and aWIPS

Deauthentication broadcast: 6  
**18**  
High Threat  
Deauthentication flood: 2  
Disasso

### Threat 360: Mac 80:E0:1D:7C:09:82

Threat Level	Threat Type	Vendor	Count	Last Reported
High	Deauthentication broadcast	Cisco Systems, Inc	1	Jul 29, 2020 12:06 pm

Location: Global/Bengaluru/BGL18/Floor4 [Full Screen](#)

Rogue AP and detecting AP don't have coordinates

### Threats (18)

Filter

Threat Level	Threat MAC address	Type
High	80:E0:1D:7C:09:82	Deauthentication broadc
High	80:E0:1D:7C:09:83	Deauthentication broadc
High	00:00:00:00:00:00	Deauthentication broadc
High	80:E0:1D:86:80:8F	Deauthentication broadc
High	F8:0B:CB:3C:30:03	Deauthentication broadc
High	00:81:C4:CD:92:7F	Deauthentication broadc
High	00:00:00:00:00:00	Deauthentication flood
High	00:81:C4:CD:92:7F	Deauthentication flood

### Detections (1) Forensic Captures (1)

Filter Download All Export

Detecting AP	Alarm ID	Capture Filename	Last Updated
AP9115_13	11	70695A7696C0_80211_1596004600648860.pcap	Jul 29, 2020 12:06 pm

AI Endpoint Analytics works for endpoints coming to Cisco DNA Center from Cisco Catalyst 9000 series access devices or a Cisco Traffic Telemetry Appliance running IOS-XE 17.3.1 or later. Additional endpoint information can optionally be retrieved from Cisco DNA Center integrated ISE, running one of (2.4.0.357 Patch 11+ or 2.6.0.156 Patch 4+ or 2.7.0.356 Patch 1+ or 3.0 onwards.

Configuration

Total Endpoints ⓘ

34

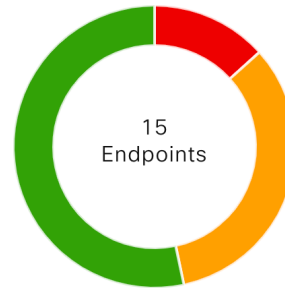


Unknown	1 (3%)
Partially Profiled	20 (59%)
Fully Profiled	13 (38%)

[View Partially Profiled Labels](#)

Trust Score *PREVIEW*

[Manage sources](#)



Low (1-3)	2 (13%)
Medium (4-6)	5 (33%)
High (7-10)	8 (53%)

AI Proposals ⓘ

Last Proposed: Nov 20, 2022 11:44 PM

Using crowdsourcing data, we were able to put together some rule proposals that could improve your profile outcomes:

- 0 New rule(s) for profiling endpoints that may be similar [Review](#)
- 0 Modification proposal(s) for previously accepted rule(s) [Review](#)
- 0 Profiling Rule(s) is/are no longer needed [Review](#)



00:50:56:B7:45:97

Hostname plz01-client Trust Score ● 3

ⓘ Two (2) unassigned profiles. [Expand](#) to show.

⚠ This endpoint has a low trust score of 3 and needs immediate attention. [View Trust Score Details](#)

Details ⚠ Trust Score Attributes

Trust Score Total: ● 3 ⓘ

### Endpoint Authentication and Compliance

> Authentication Method ● Wired802\_1x (EAP-MD5) Last Authenticated: Nov 18, 2022 04:35 PM

> Posture Not Detected

### Endpoint Anomaly Detection

> AI Spoofing Detection Not Detected

> Changed Profile Labels Not Detected

> Concurrent MAC Address ● 8 Last Scored: Oct 26, 2022 11:54 AM

> NAT Mode Detection Not Detected

> Talos IP Reputation Globally Disabled

> Unauthorized Ports Globally Disabled

# Doporučené nastavení v rámci Cisco.com

<http://cs.co/c9800-BP>



Products & Services / Wireless / Wireless LAN Controller / Cisco Catalyst 9800 Series Wireless Controllers / White Papers /

## Cisco Catalyst 9800 Series Configuration Best Practices

Updated: May 7, 2020

Contact Cisco

Table of Contents

Table of Contents

Introduction

Notes about this guide

Prerequisites

Cisco Catalyst 9800 Series ne...

Cisco Catalyst 9800 Series pro...

General controller settings

General access point settings

Network controller settings

Network access point settings

SSID/WLAN settings

Security settings

Rogue management and detec...

Share Download Print

### Introduction

The Cisco® Catalyst® 9800 Series (C9800) is the next-generation wireless LAN controller from Cisco. It combines RF excellence gained in 25 years of leading the wireless industry with Cisco IOS® XE software, a modern, modular, scalable, and secure operating system. The Catalyst Wireless solution is built on three main pillars of network excellence: Resiliency, Security, Intelligence:

Cisco Catalyst 9800 Series Wireless Controllers  
Power by Cisco IOS® XE  
Open and programmable

Cisco Catalyst 9100 Access Points  
Power by Wi-Fi technology  
Superior RF experience

Resilient



ISSU

Secure



User Define Network

Intelligent



11x Analytics

Samsung Analytics

