

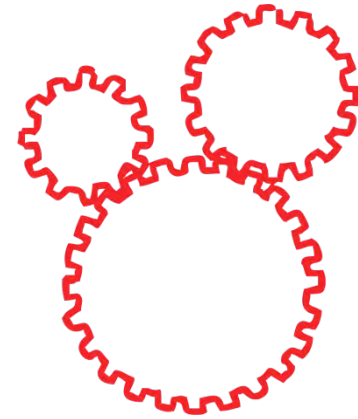
Business and technology working as one



BYOD, como protegermos

Agosto 2013

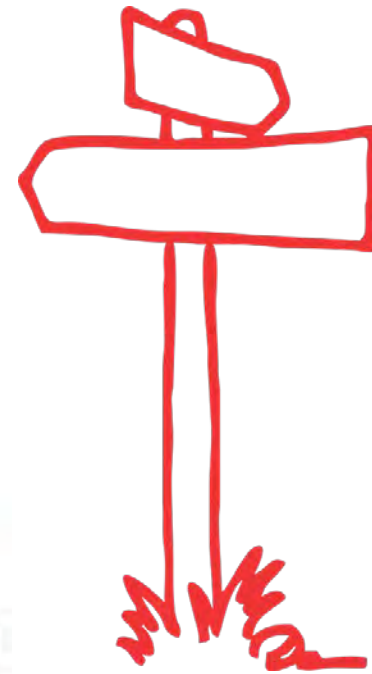
Rodrigo Coloritto



Agenda

- Introducción
- Problemática / Desafío
- Gestión
- Arquitectura
- Preguntas

Introducción



17,7%

de los empleados que llevan sus dispositivos al trabajo declaró que **TI no lo sabe**

28,4%

de los departamentos de TI **ignora** que los empleados llevan sus dispositivos al trabajo

42%

de los smartphones en el trabajo son **del empleado**

47%

empleados son **oficialmente móviles**

36%

de las empresas otorgan **privilegios de movilidad** a pedido del empleado

60%

usan para el trabajo dispositivos móviles

Por qué incorporar dispositivos a la red?

Drivers top para incorporar políticas de BYOD

- Atraer y retener talentos a través de nuevas formas de trabajo y aplicaciones personales aplicadas al trabajo diario (flexibilidad laboral)
- Aumentar la productividad como objetivo estratégico e incorporando movilidad al espacio de trabajo
- Reducir a futuro el TCO en PC y otros dispositivos sumado a bajos costos en management y fácil on boarding de nuevos empleados



Fuente: Citrix

Desafíos y expectativas



CIO

- Productividad de los empleados
- Ventajas competitivas a través de nuevas tecnologías
- TCO



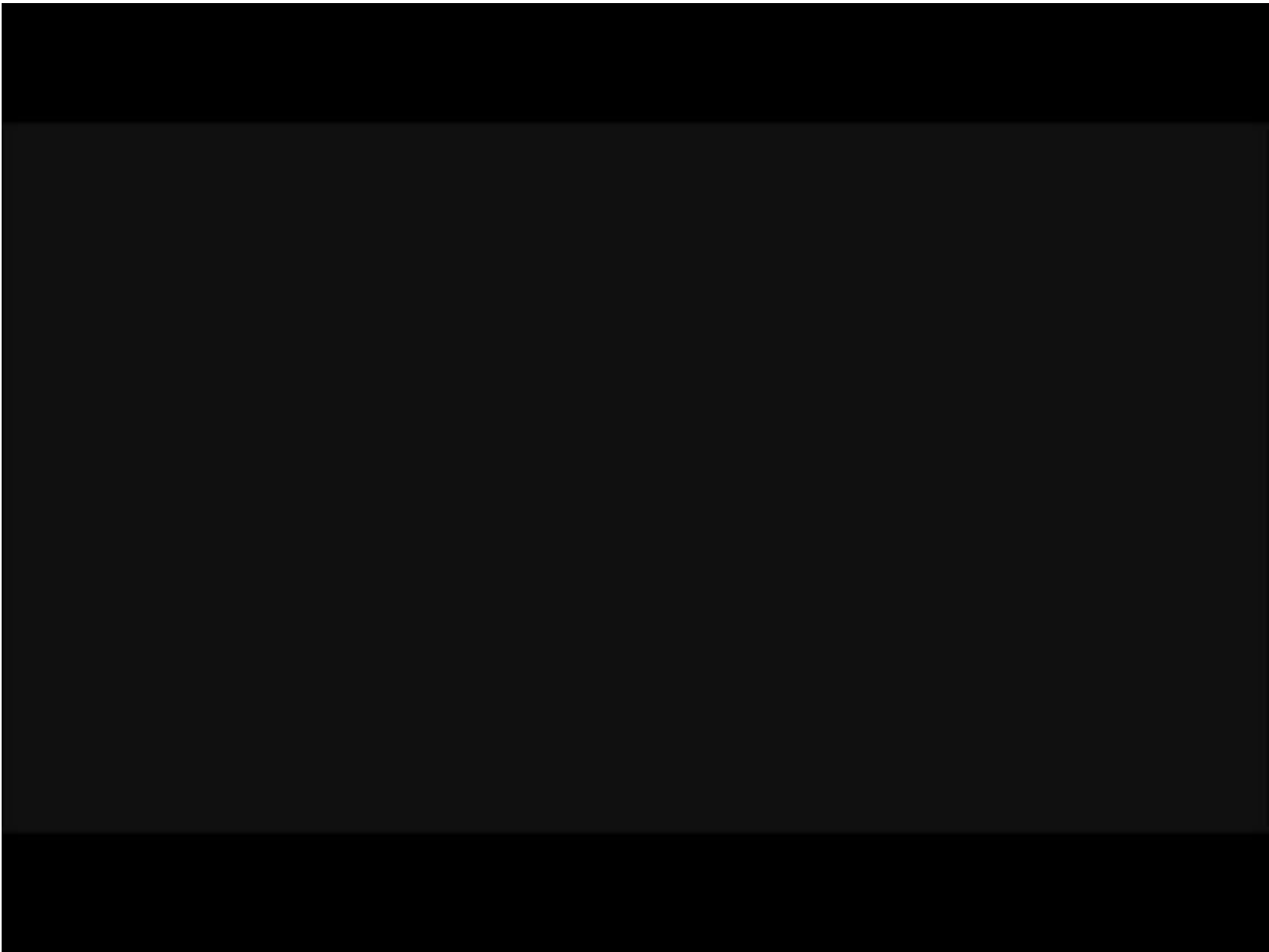
IT / Desktop Manager

- Control Management y Seguridad
- Velocidad y versatilidad en nuevos deployments

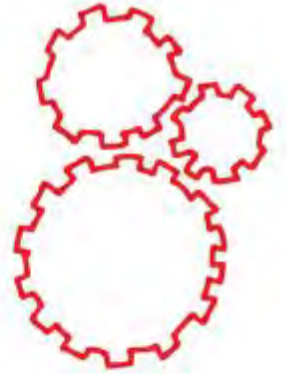


Usuario

- Experiencia en su plataforma nativa
- UE en cualquier lugar, momento y dispositivo
- Espera misma calidad dentro y fuera de la red



Problemática/Desafío



Any Device, Any Cloud



Infrastructure

Apps /
Services

Workload
s

Mobile Malware Acceleration



Android Web Malware grows

2577%

over 2012



Apps para dispositivos moviles

dSploit
The most complete and advanced IT security professional toolkit on Android.
[Download v1.0.31b](#)

AdChoices

HOME ABOUT FEATURES

Features

- WiFi Scanning & Common Router Key Cra
- Deep Inspection
- Vulnerability Search
- Multi Protocol Login Cracker
- Packet Forging with Wake On Lan Support

Hack Computers and Other Network Devices using Android

Destacado

LISTA DE REPRODU

6:49 / 6:49

Hack Computers and Other Network Devices using Android

Opensourcegangster · 83 videos

Suscribirse 21.754

108.031

852 54

Me gusta

Acerca del video Compartir Agregar a

Publicado el 21/10/2012

New colors. New look.

Samsung GALAXY S III
Designed for humans

dSploit - How to hack WI-FI passwords using android
por ECOreviewsPRO
32.627 DESTACADAS

Run Ubuntu 12.04 on Android
por Opensourcegangster
255.736 reproducciones

How to Run Backtrack 5 on Android
por Opensourcegangster
164.822 reproducciones

Networking Hacking Tools for Android
por Opensourcegangster
124.145 reproducciones

How To Crack Lockscreen Pattern on

La primer reacción



Administración de Dispositivos Móviles

- Gestión de Dispositivo movil
- Monitoreo y reportes
- Control de Inventário
- Configuración
- Seguridad

Información sobre los dispositivos

re90190z iPad

Comandos Rápidos

Resumo Conformidade Perfis Aplicativos Conteúdo Certificados Usuário GPS Log de eventos

Segurança

- Comprometimento ✓
- Garanciado(s) ✓
- Proteção de dados ✓
- Criptografia de bloco ✓
- Criptografia de arquivo ✓

Código de acesso

- Código de acesso ✓
- Conformidade do código de acesso ✓
- Conformidade de perfil de código de acesso ✓

Rede

- Status do cartão SIM ✓
- Status de roaming ⚠
- Roaming dos dados ⚠

Perfis

- 5 Instalado(s) ⚠
- 1 Não instalado(s) ⚠

Certificados

- 1 Instalado(s) ⚠

Aplicativos

- 63 Instalado(s) ⚠

Conteúdo

- 0 Instalado(s) ⚠
- 4 Atribuído(s) ⚠

Status

- Inscrito(s) ✓

Visto pela última vez

05/05/2013 11:50:00

Data de registro

03/05/2013 08:49:29

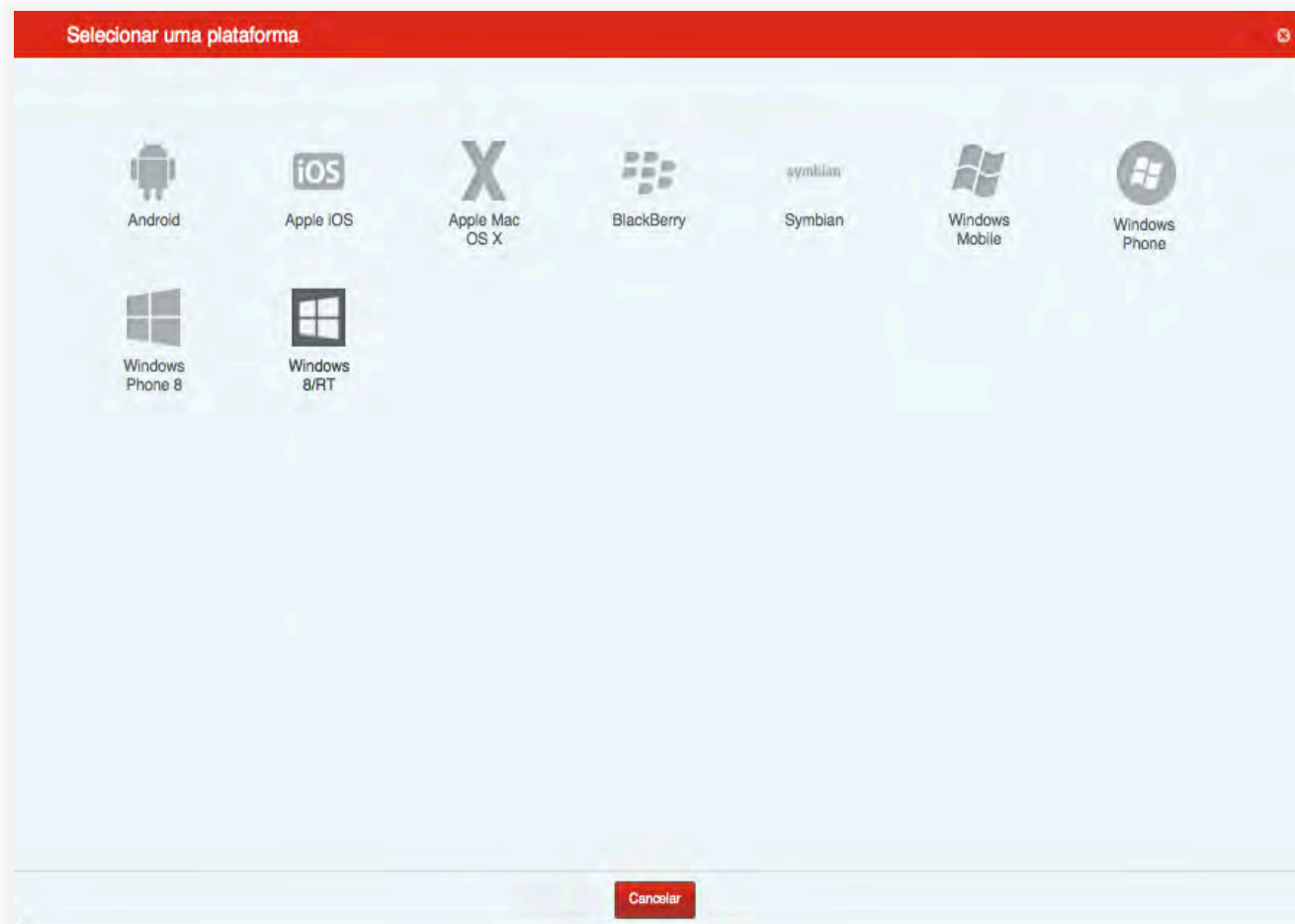
UDID

E4F5199AA52F6E273CA2CEC
19524212C206CBF21

Número de série

DMPHK9DEDVGL

Plataformas soportadas



Dashboard

Grupo de organização

Oferta

Painel

Rastreamento de dispositivos

Conformidade do dispositivo

Gerenciamento de e-mail

Status de inscrição

Avançado

Grupos de organização

Conformidade do dispositivo

Dispositivos comprometido

Em conformidade Fora de conformidade
Desconhecido(a)



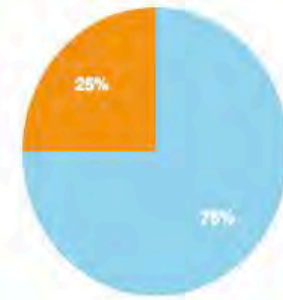
Utilizando código de acesso

Em conformidade Fora de conformidade
Desconhecido(a)



Criptografia

Em conformidade Fora de conformidade
Não aplicável



↑ Detecta dispositivos “Jailbreak”
o “Rooted”

Todos(as)

Filtro de pesquisa



Visto pela última vez	Apelido	D/C/F	Usuário	Nome de exibição	Plataforma	Modelo	Grupo de organização	Inscri
▲ 32 m	re90190z iPhone		re90190z	Luiz Nonato	Apple	iPhone	Oferta	Inscrib
▲ 1 h	re90190z Android	C	re90190z	Luiz Nonato	Android	Android	Oferta	Inscrib
▼ 1 d	re90190z iPad		re90190z	Luiz Nonato	Apple	iPad	Oferta	Inscrib
▼ 41 d	iPad Oferta	C	oferta.promonlogicalis	Oferta PromonLogicalis	Apple	iPad	Oferta	Inscrib

Itens 1-4 de 4

Itens por página: 50

Simplificar el Onboarding

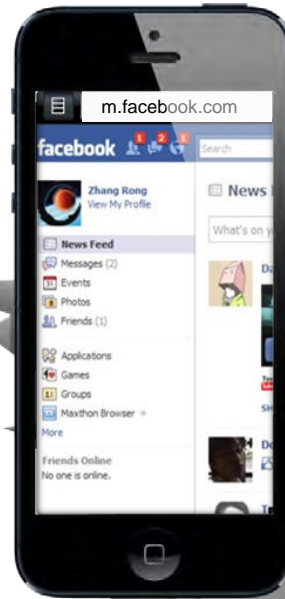


La brecha móvil...

Móviles nativas



Navegador Web móvil



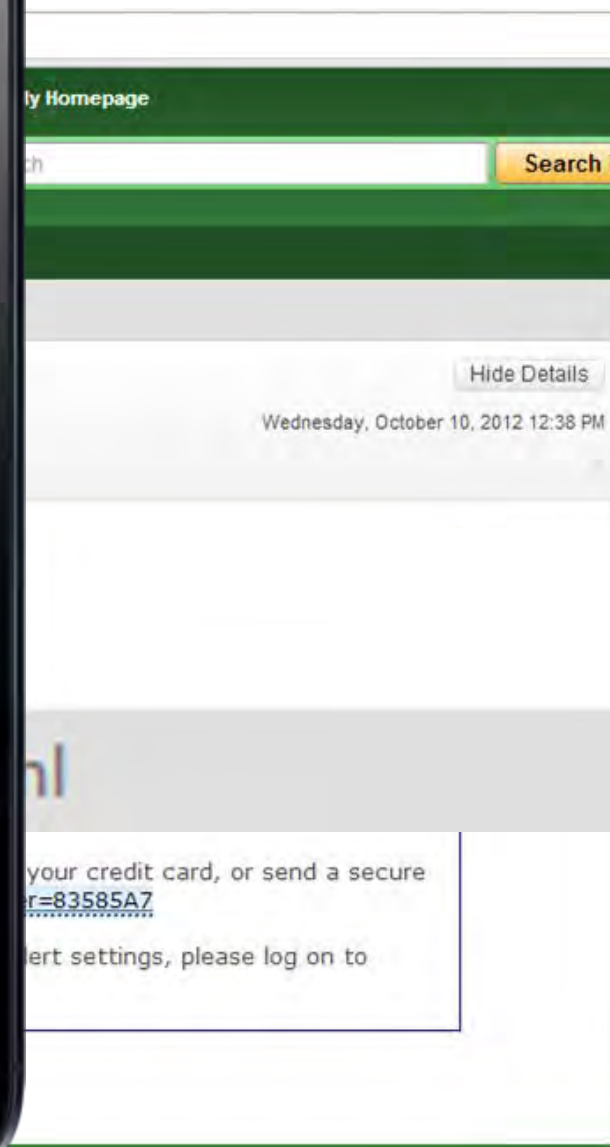
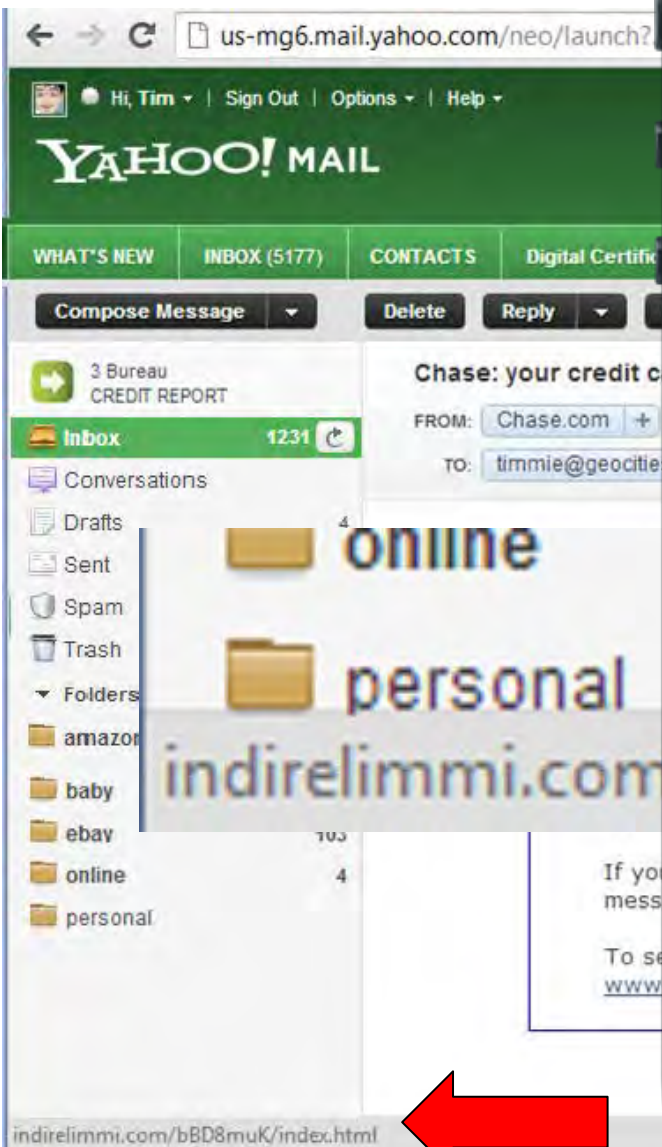
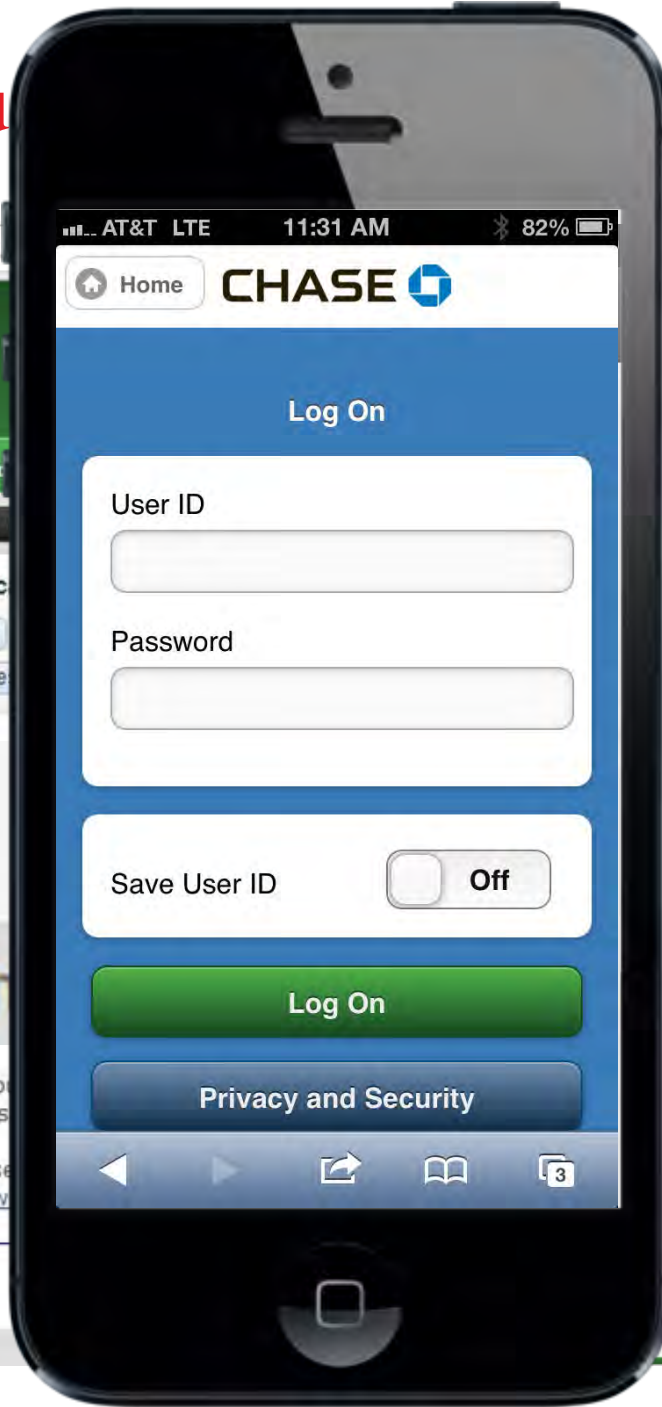
Navegador Web de Escritorio



Brecha de App Móvil

Amenazas Comu

licaciones



Necesidad de Control Granular

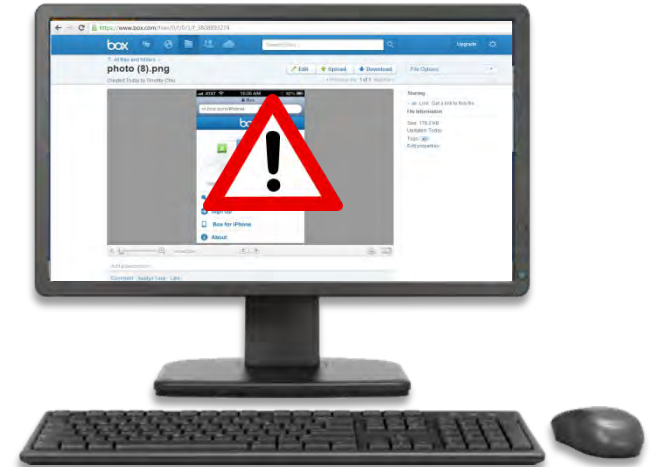
Nativa



Navegador Web Móvil



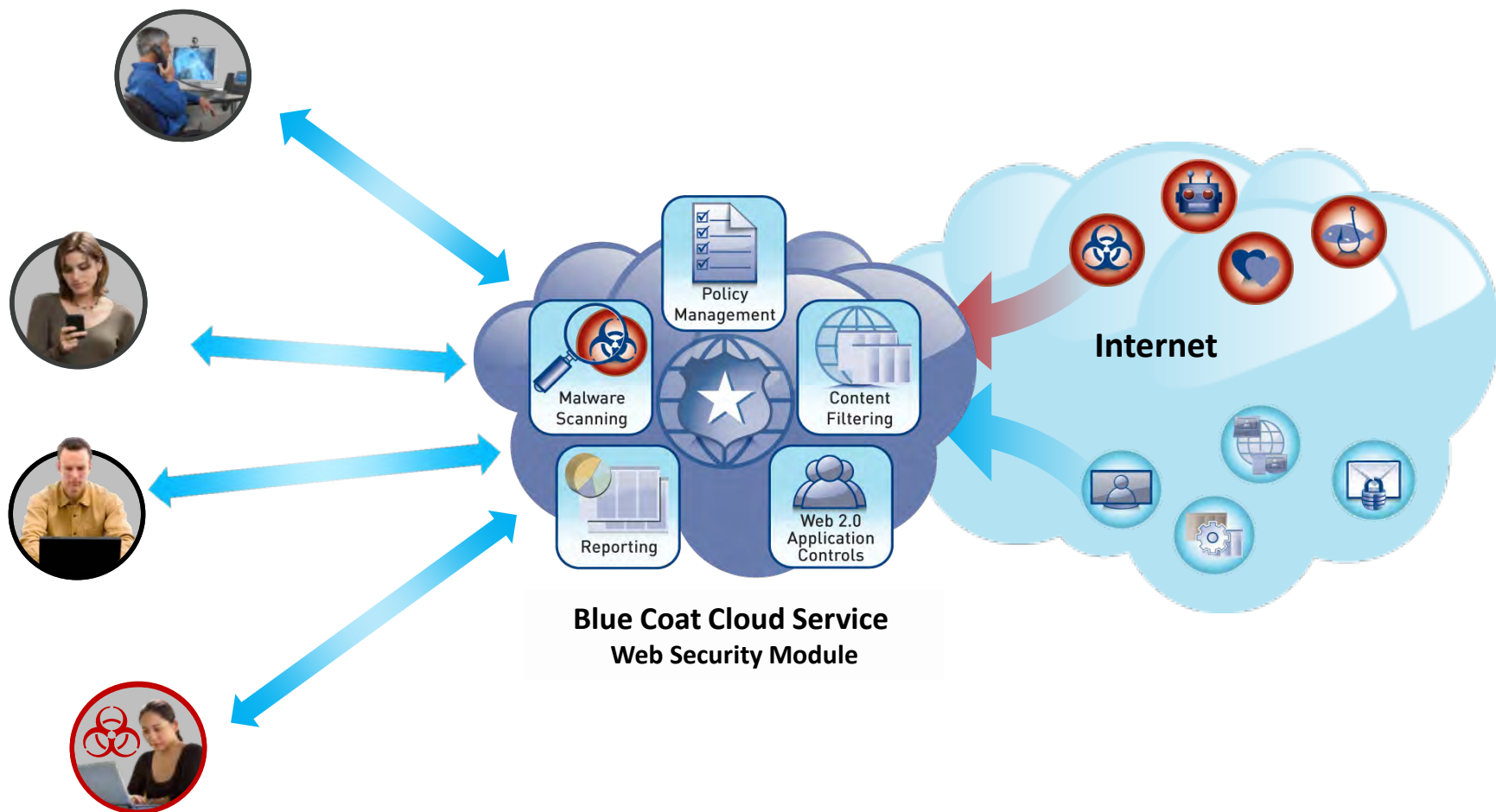
Navegador Web de Escritorio



- Políticas de seguridad en todo tipo de aplicaciones
- Control granular que distinga entre diferentes tipos de aplicaciones

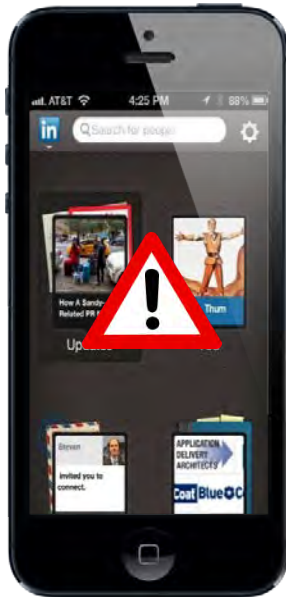


Solución end to end (web security)



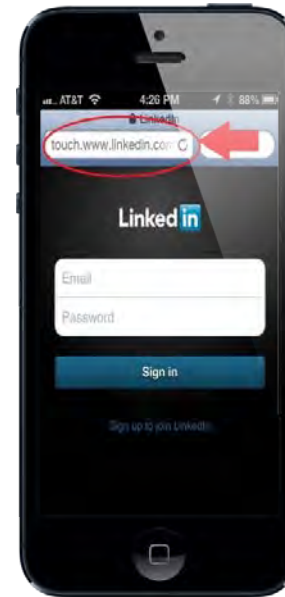
El complemento de un MDM

App Nativa



- MDM controla qué apps pueden instalarse
- Control binario (on/off switch) de apps permitidas

Mobile Web Browser



- Navegador web abre la puerta a apps descontroladas
- Sobrepasa controles binarios del MDM

Arquitectura/Solución



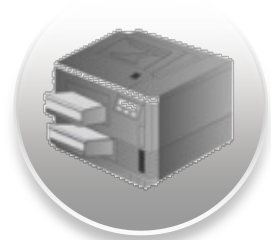
Controlar el acceso – CISCO ISE



autenticación



autorización

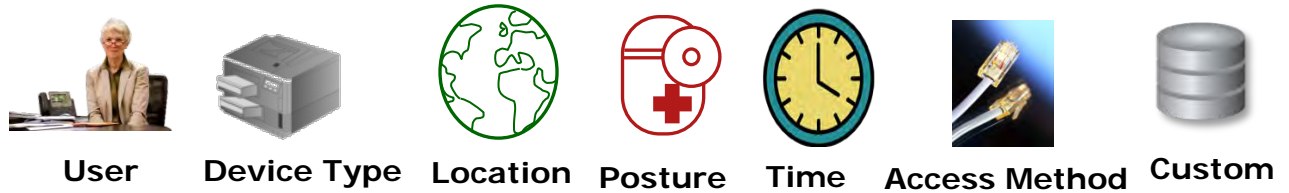


profiling



invitados

Flexibilidad y control



Authorization Policy At A Glance

First Matched Rule Applies

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
Enabled	Game_Console	Game_Console-Registered		Game_Console
Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers AND San Jose	AD_Login
Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant AND MATCHES [0-5]	Employee_Wireless
Enabled	Employee-iPAD	Apple-iPad	Employee_Wireless AND Posture_Compliant AND North_America	Employee_iPAD
Enabled	Contractor-iPAD	Android OR Apple-iPad OR Apple-iphone OR Apple-iPod OR BlackBerry	Contractor_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
Disabled	Default-Posture	Any		CWA_Posture_Remediation
Enabled	Default	Any		Central_Web_Auth

ISE Perfilado

■ Que es “ISE Profiling”:

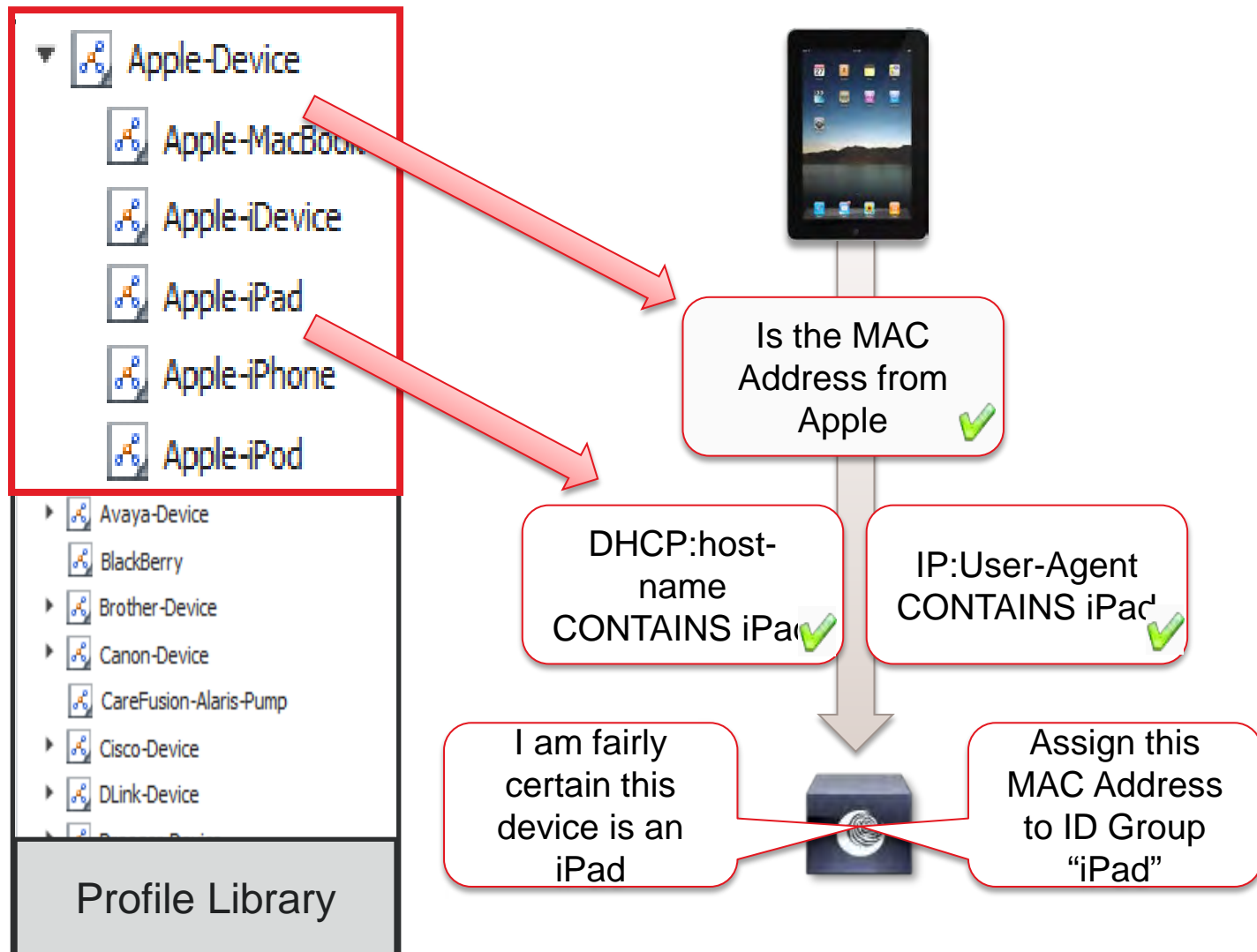
- Clasificación dinámica de todos los dispositivos conectados a la infraestructura de networking.
- Provee información de “qué” está conectado independientemente de la identidad del usuario y la politica de uso asocicada.



PCs	Non-PCs			
	UPS	Phone	Printer	AP

Políticas de Perfilado

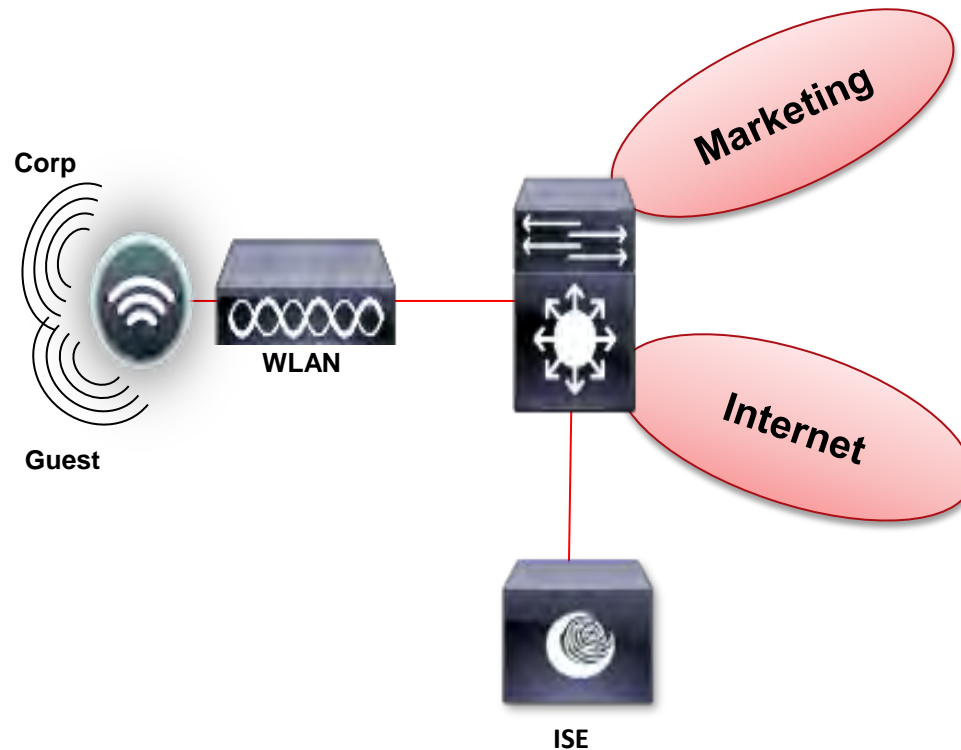
Combinar características del dispositivo para generar políticas de uso.



Perfilado de dispositivos de usuarios

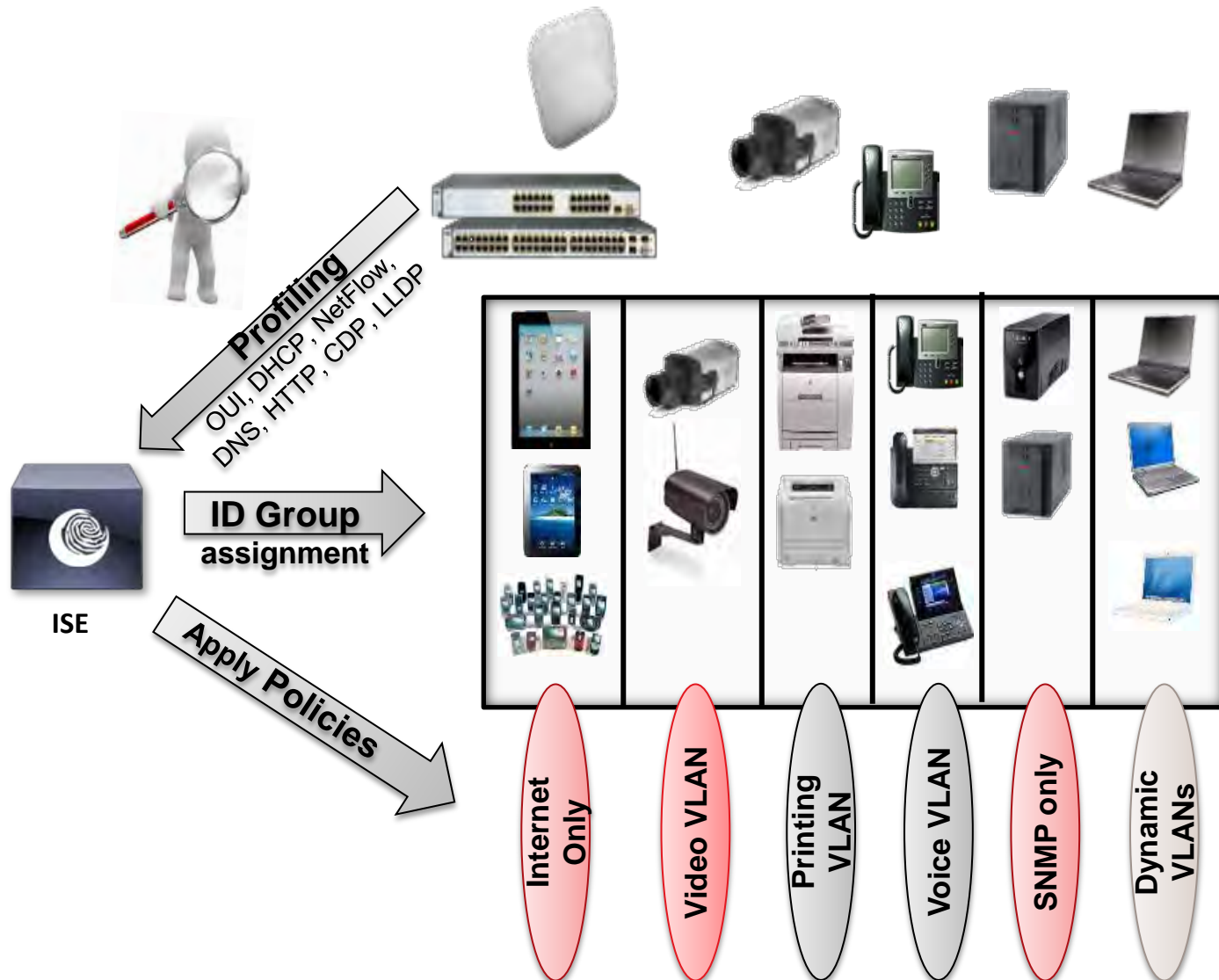
Differentiated Access Based on Device Type

**Kathy + Corp
Laptop = Full
Access to
Marketing VLAN**



**Kathy + Personal
Tablet /
Smartphone
= Limited Access
(Internet Only)**

Perfilado - Resumen



Acceso Invitado



Identity Services Engine
Guest Portal

Username:

Password:

Login

[Self Service](#)
[Change Password](#)
[Device Registration](#)

© 2011, Cisco Systems, Inc. All rights reserved

ISE – Sponsor Portal

Account Management > View All Guest Accounts > Create Guest Account

Create Guest Account

First Name:

Last Name:

* Email Address:

Phone Number:

Company:

* Group Role:

* Time Profile:

* Timezone:

* Language Template for Email/SMS Notifications:

* = Required fields

Layout flexible

- Se definen campos obligatorios u opcionales
- Se pueden agregar hasta 5 atributos parametrizables

Roles de invitado y horarios

- Templates pre-definidos por el administrador

Sponsor Portal: Informando al invitado

CISCO Sponsor Portal

Account Management > View All Guest Accounts > Create Guest Account

Successfully Created Guest Account: mbole@cisco.com

Username: mbole@cisco.com
Password: adc
First Name: Muriel
Last Name: Bole
Email Address: mbole@cisco.com

Phone Number:
Company: cisco
Status: AWAITING INITIAL LOGIN
Suspended: false
Group Role: Guest
Time Profile: custom

Timezone: Europe/London
Account Start Date: 2011-10-13 16:00:00 BST
Account Expiration Date: 2011-10-14 16:00:00 BST

Email SMS Print Create Another Account View All Accounts

Username

- Puede ser una combinación del nombre y apellido o del email.

Password

- Generación automática (o no)
- Grado de complejidad configurable

Experiencia usuario invitado

The image shows two overlapping screenshots of the Cisco Identity Services Engine 1.1 Guest Portal. The top screenshot displays the 'Acceptable use policy' page, which includes a list of terms and conditions and an 'Accept' button. The bottom screenshot shows a 'Login Successful' message with an 'EXIT' button.

Identity Services Engine 1.1 Guest Portal
john@cisco.com Logout About

Acceptable use policy

Please accept the policy:

1. You are responsible for
 - maintaining the confidentiality of the password and
 - all activities that occur under your username and password.
2. 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 unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.
3. Cisco Systems reserves the right to suspend the Service if
 - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
 - you are using the Service for criminal or illegal activities.
4. You do not have the right to resell this Service to a third party.
5. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept terms and conditions

Accept Decline

Identity Services Engine

Login Successful
Please retry your original URL request.

EXIT

ISE - My Devices Portal

Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

* Device ID

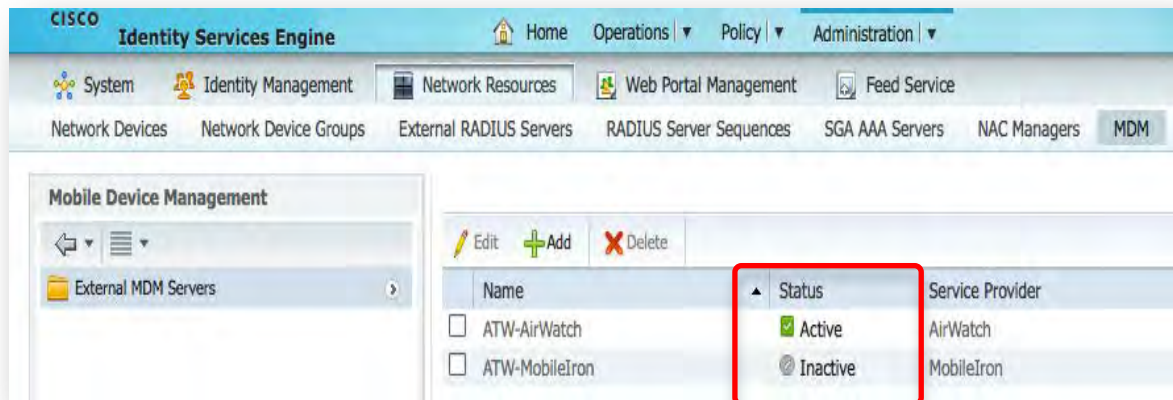
Description

Warning: Marking this device as lost will remove it from the network and lock it out until reinstated via this portal. Are you sure you would like to proceed?

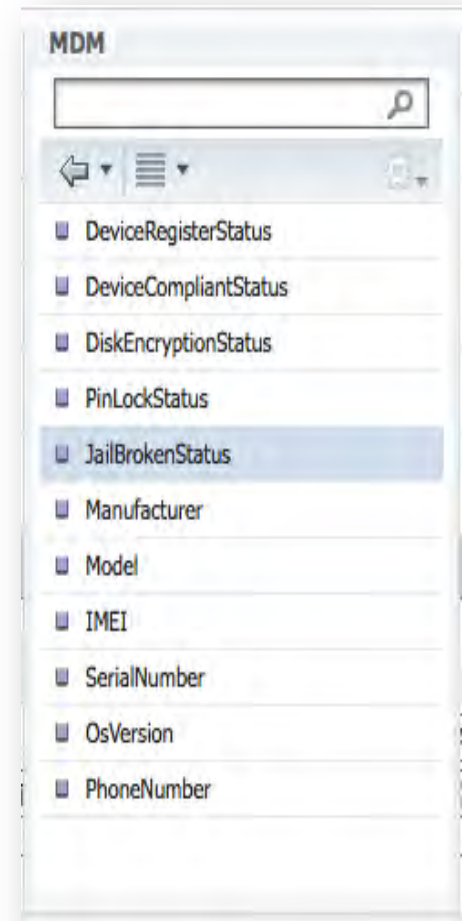
Your Devices

State	Device ID	Description	Action
...	00:11:22:33:44:55	My Windows Laptop	Edit <input type="button" value="Lost?"/>
...	11:22:33:44:55:66	My iPad	Edit <input type="button" value="Lost?"/>
✖	22:33:44:55:66:77	My Android Phone	Edit <input type="button" value="Reinstate"/>

Integración con sistemas de MDM



Attributes from MDM



Version: 5.0



Version 6.2



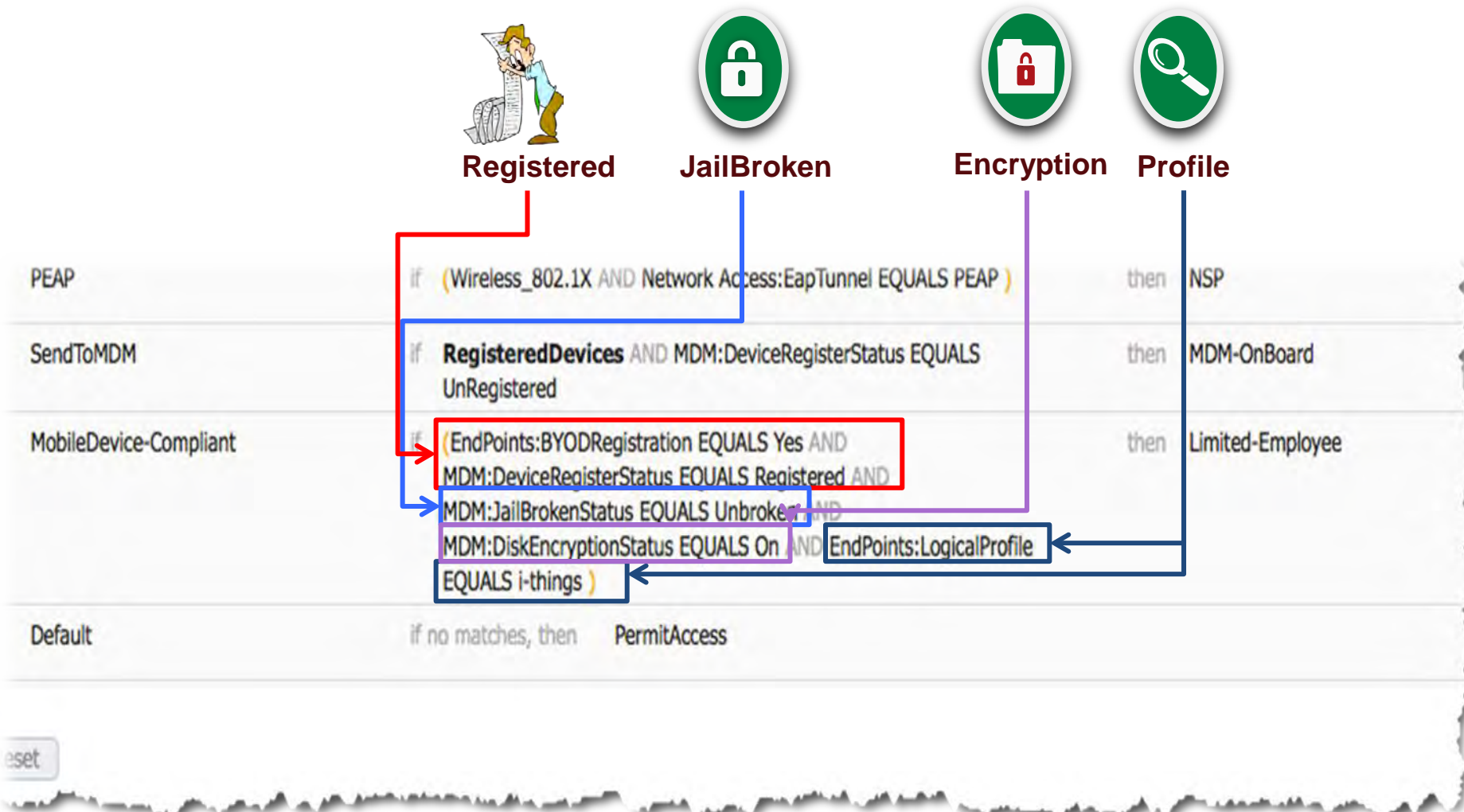
Version: 7.1



Version: 2.3

Integración con sistemas de MDM

Nuevos atributos en las reglas de acceso



reset

Integración con sistemas de MDM

Funciones adicionales en el portal

The image shows a screenshot of the Cisco My Devices Portal. The top left features the Cisco logo and the text "CISCO My Devices Portal". Below this is a section titled "Add a New Device" with a sub-instruction: "To add a device, enter the Device ID and description and click Submit." The main content area displays a table of devices. A red box highlights the "MDM Actions" dropdown menu in the top right, which lists "Full Wipe", "Corporate Wipe", and "PIN Lock". Another red box highlights the action buttons for a specific device in the table: "Edit", "Reinstate", "Lost?", "Delete", "Full Wipe", "Corporate Wipe", and "PIN Lock". A red arrow points from the "Full Wipe" option in the dropdown menu to the "Full Wipe" button in the table. A legend box on the right lists the actions: Edit, Reinstate, Lost?, Delete, Full Wipe, Corporate Wipe, and PIN Lock.

Endpoints

Edit + Add X Delete Import Export MDM Actions

Endpoint Profile

- Android
- Android
- Android
- Android

MAC F4:00:00:00:00:00

00:13:76:96:C1:54

00:23:76:95:86:93

00:18:A4:06:71:4F

Add a New Device

To add a device, enter the Device ID and description and click Submit.

Our devices

Edit Reinstate Lost? Delete Full Wipe Corporate Wipe PIN Lock

Select	Device ID	Description	State
<input type="radio"/>	CC:CC:12:34:15:CC		

- Edit
- Reinstate
- Lost?
- Delete
- Full Wipe
- Corporate Wipe
- PIN Lock

Reportes más completos

Failure Reason
Phone is out of contact; Device administrator is deactivated; Password not set

Identity Services Engine

Mobile Device Management

From 12/02/2012 12:00:00 AM to 12/31/2012 11:59:59 PM

Logged At	Server	Username	MAC Address	IP Address	Session ID	OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model	IMEI	Serial Number	Phone Number	Failure Reason
2012-12-20 18:00:03.506	se-mdm		7C-60-62-E3-05-05		0a012c5a000001e55039ad	iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact; Device administrator is deactivated; Password not set
2012-12-20 01:19:27.913	se-mdm		7C-60-62-E3-05-05		0a012c5a000001a95012678c	iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact; Device administrator is deactivated; Password not set
2012-12-20 00:36:34.817	se-mdm		7C-60-62-E3-05-05		0a012c5a000001a050d25e9c	iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:29.481	se-mdm		7C-60-62-E3-05-05		0a012c5a000001a050d25e9c	iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:27.081	se-mdm		7C-60-62-E3-05-05		0a012c5a0000019350d23f2d	iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-19 01:13:12.138	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 01:13:00.02	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:57:00.015	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	Device is not registered with MDM
2012-12-19 00:49:29.929	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	Device is not registered with MDM
2012-12-19 00:46:49.153	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	Device is not registered with MDM
2012-12-19 00:42:30.46	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:37:33.096	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:36:50.083	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:26:26.935	se-mdm		8C-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3	

OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model	IMEI	Serial Number	Phone Number
iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	🔒	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
Android 4.0	✓	✓	🔒	✓	✓	samsung	GT-P5113			PDA 3

Powerful Search

CISCO Identity Services Engine
npf-sjca-pap02 | Imbashir | Logout | Feedback

Setup Assistant

Home Operations Policy Administration

Metrics

Total Endpoints: 1,599
Active Endpoints: 359
Active Guests: 0
Profiled Endpoints: 131
Posture Compliance: 88%

System Summary

Name	Utilization and Latency 24h		
	CPU	Memory	Latency
bx22-11a-pdp1			
npf-hyd04-pdp04			
npf-sjca-lpep01	No Data Av.	No Data Av.	No Data Av.
npf-sjca-lpep02	No Data Av.	No Data Av.	No Data Av.
npf-sjca-mnt01			
npf-sjca-mnt02			
npf-sjca-pap02			

Alarms

Name	Occurrences	Last Occurred
Configuration Changed	4414 times	18 mins ago
COA Failed	558 times	53 mins ago
Health Status Unavailable	300 times	1 hr 41 mins ago
Health Status Unavailable	300 times	1 hr 41 mins ago
RADIUS Request Dropped	3168 times	1 hr 42 mins ago
RADIUS Request Dropped	3168 times	1 hr 42 mins ago
NTP Sync Failure	638 times	1 hr 50 mins ago
License Violation	167 times	1 hr 56 mins ago

Authentications

Passed: 11,418
Failed: 35,845

Distribution By:

- Identity Store: 4
- Identity Group: 9+
- Network Devic...: 3
- Location: 8
- Failure Reason: 9+

Profiler Activity

Total: 96

Distribution By:

- Endpoint Profile: 9+
- Identity Group: 5

Posture Compliance

Total: 79

Distribution By:

- Posture Status: 1
- Operating Syst...: 4



System Summary

Name	Utilization and L...	
	CPU	Mem
bx22-11a-pdp1		
npf-hyd04-pdp04		
npf-sjca-lpep01	No Data Avr	No Data
npf-sjca-lpep02	No Data Avr	No Data
npf-sjca-mnt01		
npf-sjca-mnt02		
npf-sjca-pap02		

npf-sjca-pap02 | imbashir | Logout | Feedback

imran

Profiled Endpoints

131

24h

Authentications

Suggestions

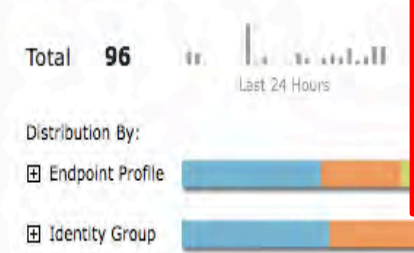
Authorization Profile

- wlc_sjcm_imran_prepostu re

Username

- imran

Profiler Activity



Metrics

Total Endpoints
1,601

System Summary

Name	CPU
bxb22-11a-pdp1	
npf-hyd04-pdp04	
npf-sjca-lpep01	No Data Av
npf-sjca-lpep02	No Data Av
npf-sjca-mnt01	
npf-sjca-mnt02	
npf-sjca-pap02	

Profiler Activity

Total **96** Last 24 H

Distribution By:

- Endpoint Profile
- Identity Group

Search

3 Connected | **0** Failed | **1** Disconnected | **4** Total

Distribution

- ▶ Authorization Profile (2)
- ▶ Endpoint Profile (4)
- ▶ Identity Group (1)
- ▶ Identity Store (2)
- ▶ Location (1)
- ▶ Network Device (2)
- ▶ Network Device Type (1)
- ▶ Posture Status (1)
- ▶ User Type (1)

- Apple-iPad**

imran, D0:23:DB:E1:B1:B9, 10.34.79.10

SJC#SJCM1, Wireless#W... NSP-Permit-Access
- Windows7-Workstation**

imran, 1C:65:9D:38:5B:19, 10.34.84.137

SJC#SJCM1, Wireless#W... WLC_SJCM_V603
- OS_X-Workstation**

imran, 14:10:9F:E8:F1:80, 10.34.84.135

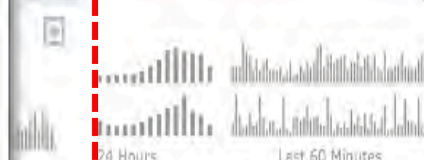
SJC#SJCM1, Wireless#W... WLC_SJCM_V603
- Apple-iPhone**

imran, 9C:20:7B:17:A3:91, -

SJC#SJCM1, Wireless#W... NSP-Permit-Access

Export Results

Posture Compliance
88%



Metrics

Total Endpoints
1,601

System Summary

Name	U	CPU
<input checked="" type="checkbox"/> bxb22-11a-pdp1		
<input checked="" type="checkbox"/> npf-hyd04-pdp04		
<input checked="" type="checkbox"/> npf-sjca-lpep01	No Data Av	
<input checked="" type="checkbox"/> npf-sjca-lpep02	No Data Av	
<input checked="" type="checkbox"/> npf-sjca-mnt01		
<input checked="" type="checkbox"/> npf-sjca-mnt02		
<input checked="" type="checkbox"/> npf-sjca-pap02		

Profiler Activity

Total **96** Last 24 H

Distribution By:

- Endpoint Profile
- Identity Group

Search

3 Connected | **0** Failed | **1** Disconnected | **4** Total

Distribution

- ▶ Authorization Profile (2)
- ▶ Endpoint Profile (4)
- ▶ Identity Group (1)
- ▶ Identity Store (2)
- ▶ Location (1)
- ▶ Network Device (2)
- ▶ Network Device Type (1)
- ▶ Posture Status (1)
- ▶ User Type (1)

Apple-IPad ✓

 imran, D0:23:DB:E1:B1:B9, 10.34.79.10
SJC#SJCM1, Wireless#W... NSP-Permit-Access

Windows7-Workstation ✓

 imran, 1C:65:9D:38:5B:19, 10.34.84.137
SJC#SJCM1, Wireless#W... WLC_SJCM_V603

OS_X-Workstation ✓

 imran, 14:10:9F:E8:F1:80, 10.34.84.135
SJC#SJCM1, Wireless#W... WLC_SJCM_V603

Apple-iPhone ⌚

 imran, 9C:20:7B:17:A3:91, -
SJC#SJCM1, Wireless#W... NSP-Permit-Access

Export Results

Posture Compliance
88%



Session Trace

Endpoint Details | Search Results

Metrics

Total Endpoints

1,601

System Summary

Name	CPU	UP
bx22-11a-pdp1		
npf-hyd04-pdp04		
npf-sjca-lpep01	No Data Av	
npf-sjca-lpep02	No Data Av	
npf-sjca-mnt01		
npf-sjca-mnt02		
npf-sjca-pap02		

Profiler Activity

Total **96** Last 24 H

Distribution By:

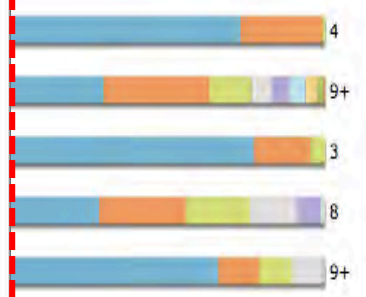
- Endpoint Profile
- Identity Group

03/14 15:12:18.000	03/14 15:12:32.000	03/14 15:37:40.000
Profiled (Apple-iPad)	Authenticated & Authorized (NSP-Permit-Access)	Re-Auth (NSP-Permit-Access)
Profiled (Apple-iPad)	Authenticated & Authorized (NSP-Permit-Access)	Authenticated & Authorized (NSP-Permit-Access) Mar 14, 13 03:12:32.000 PM
80002 Profiler EndPoint profiling event occurred		
Authenticated & Authorized (NSP-Permit-Access)	03/14 15:12:32.000	
11001 : Received RADIUS Access-Request		
11017 : RADIUS created a new session		
15049 : Evaluating Policy Group		
15008 : Evaluating Service Selection Policy		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15004 : Matched rule		
11507 : Extracted EAP-Response/Identity		

Posture Compliance

88%

24h



Session Trace

Endpoint Details

Search Results

Metrics

Total Endpoints
1,601

System Summary

Name	UP	CPU
bxb22-11a-pdp1		
npf-hyd04-pdp04		
npf-sjca-lpep01	No Data Av	
npf-sjca-lpep02	No Data Av	
npf-sjca-mnt01		
npf-sjca-mnt02		
npf-sjca-pap02		

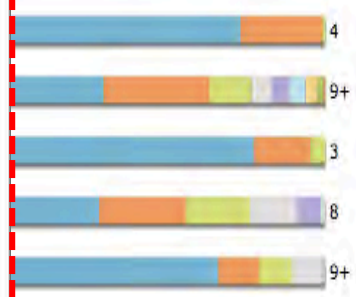
Profiler Activity

Total **96** Last 24 H

- Distribution By:
- Endpoint Profile
 - Identity Group

03/14 15:12:18.000	03/14 15:12:32.000	03/14 15:37:40.000
Profiled (Apple-iPad)	Authenticated & Authorized (NSP-Permit-Access)	Re-Auth Authenticated & Authorized (NSP-Permit-Access) Mar 14, 13 03:12:32.000 PM
Profiled (Apple-iPad)		
80002 Profiler EndPoint profiling event occurred		
Authenticated & Authorized (NSP-Permit-Access)	03/14 15:12:32.000	
11001 : Received RADIUS Access-Request		
11017 : RADIUS created a new session		
15049 : Evaluating Policy Group		
15008 : Evaluating Service Selection Policy		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15048 : Queried PIP		
15004 : Matched rule		
11507 : Extracted EAP-Response/Identity		

Posture Compliance
88%



Export Results

Endpoint Details

Session Trace

Search Results

Authentication

Accounting

Profiler

Details | Result | Other Attributes | Steps

Name

Value

Source Timestamp	2013-03-14 15:37:40.778
Received Timestamp	2013-03-14 15:37:40.848
Policy Server	npf-sjca-pdp02
Event	5200 Authentication succeeded
Username	imran
User Type	
Endpoint Id	D0:23:DB:E1:B1:B9
IP Address	
Identity Store	
Identity Group	RegisteredDevices
Audit Session Id	0a224cd4000011df51424b90
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	sjcm-00a-npf-wlc1

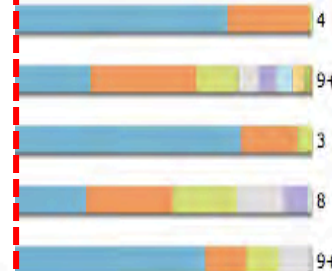
imran

Setup Assistant

Posture Compliance

88%

24h



Metrics

Total Endpoints

1,601

System Summary

	Name	Utiliz
		CPU
<input checked="" type="checkbox"/>	bx22-11a-pdp1	
<input checked="" type="checkbox"/>	npf-hyd04-pdp04	
<input checked="" type="checkbox"/>	npf-sjca-lpep01	No Data Avr
<input checked="" type="checkbox"/>	npf-sjca-lpep02	No Data Avr
<input checked="" type="checkbox"/>	npf-sjca-mnt01	
<input checked="" type="checkbox"/>	npf-sjca-mnt02	
<input checked="" type="checkbox"/>	npf-sjca-pap02	

Profiler Activity

Total 96 Last 24 Hour

Distribution By:



Export Results

Control Manual

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Home', 'Operations', 'Policy', and 'Administration' menus. Below this, there are tabs for 'Authentications', 'Reports', 'Endpoint Protection Service', and 'Troubleshoot'. The main content area displays a table of active sessions. The table has columns for 'Initiated', 'Updated', 'Session Status', 'CoA Action', 'Endpoint ID', 'Identity', 'IP Address', 'Endpoint Profile', 'Posture Status', 'Server', 'Auth Method', and 'Authentication Protocol'. A red box highlights the 'CoA Action' dropdown menu for a session with ID '00:50:56:87:00:04'. The dropdown menu shows two options: 'Session reauthentication' and 'Session termination'. A red arrow points from a text box below to this menu.

Initiated	Updated	Session Status	CoA Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	Server	Auth Method	Authentication Protocol
Oct 01 8:48:25.588 PM	Oct 01 8:48:26.555 PM	Started	⌵	00:50:56:87:00:04	employee1	10.1.10.50		Pending	atw-cp-ise01	mab	Lookup
Oct 01 8:39:46.212 PM	Oct 01 8:39:47.258 PM	Started			employee1	10.1.41.102	Android	Pending	atw-cp-ise01	dot1x	PEAP (EAP-MSCHAPv2)

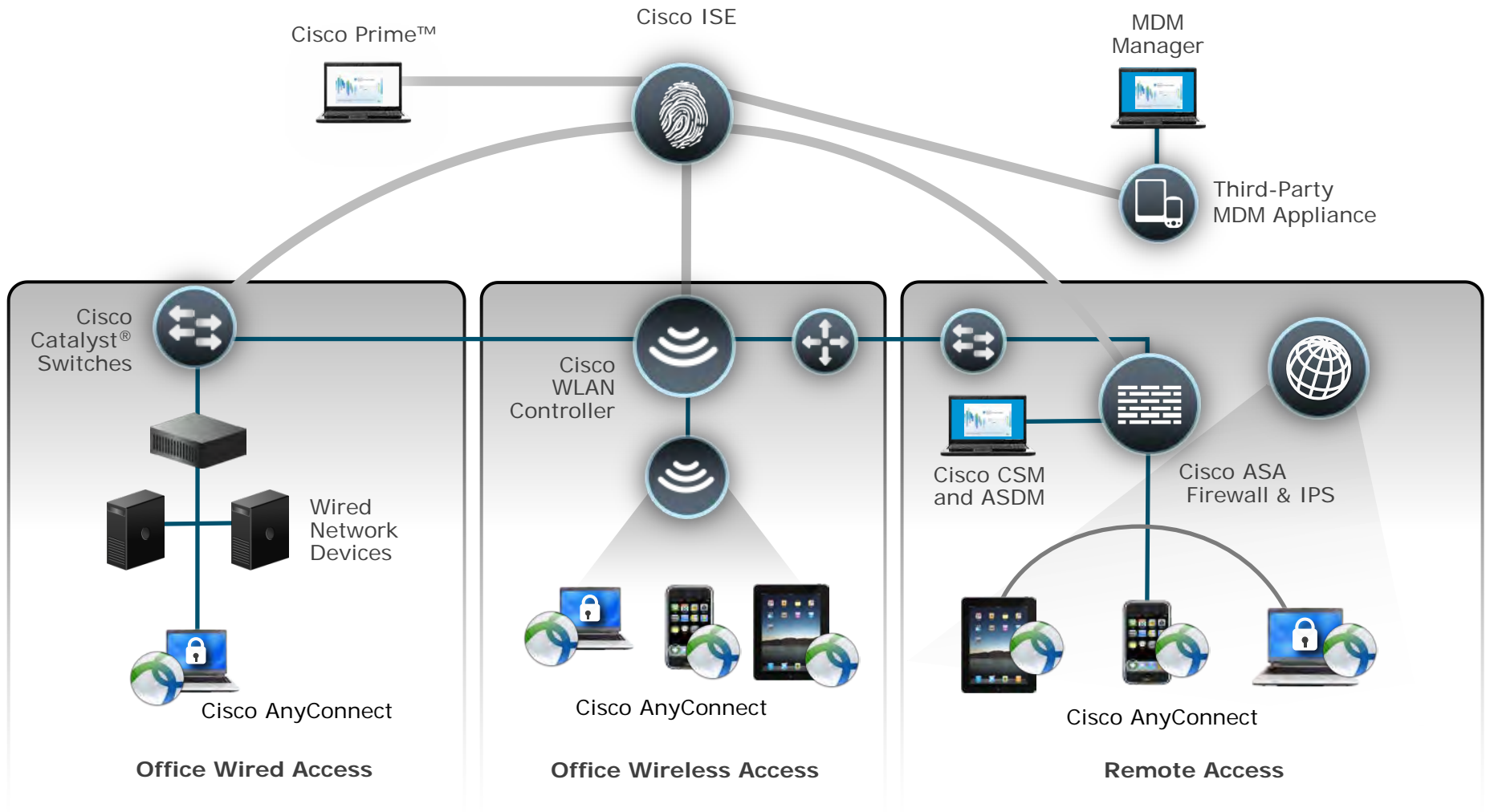
Forzar a re-autenticar

■ Politica unificada en toda la empresa

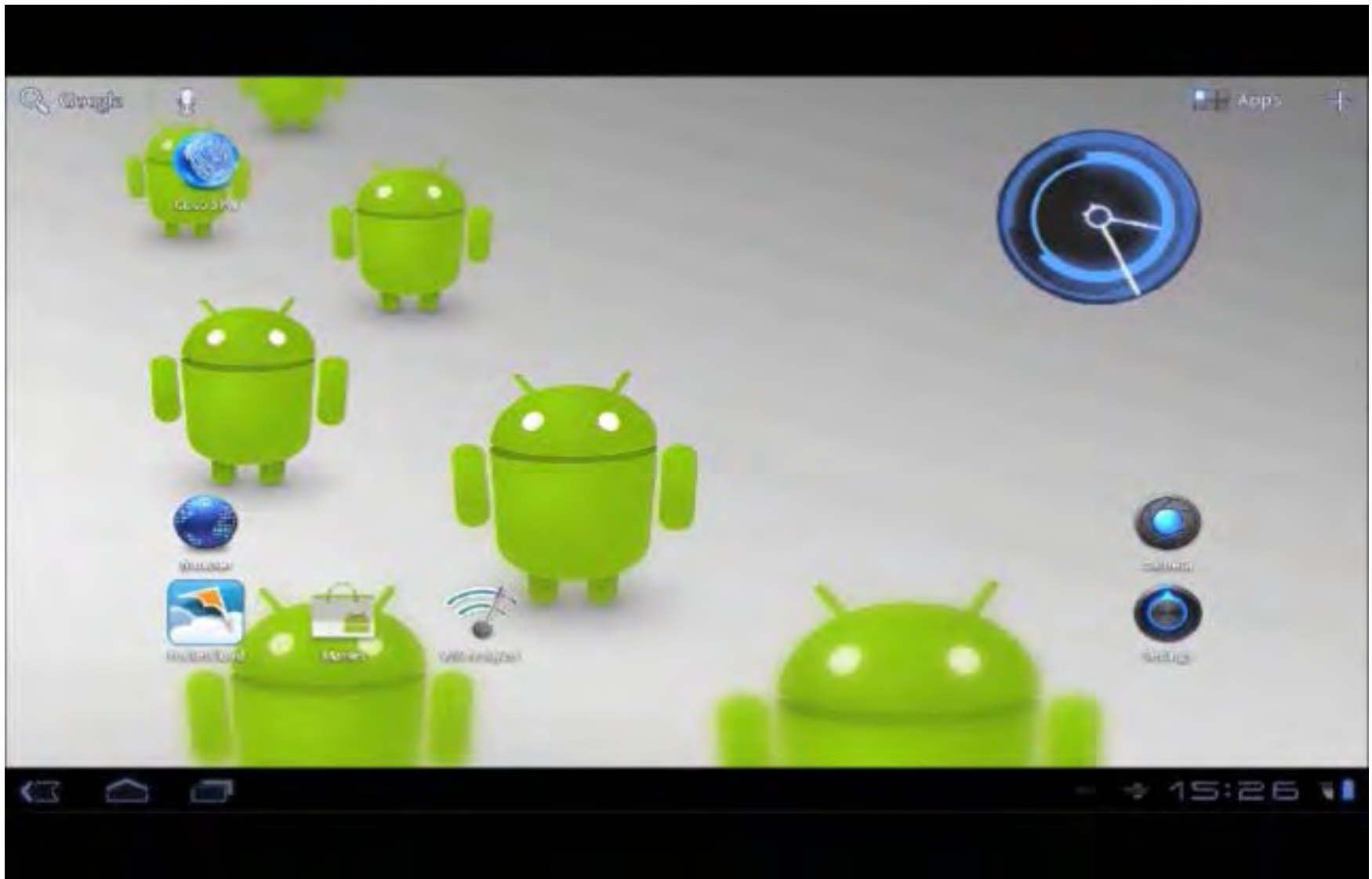


Identity (802.1X)-Enabled Network

Acceso Seguro Unificado



Experiencia del usuario corporativo



A black and white photograph of a man in a light-colored suit and patterned tie, holding a tablet. The tablet displays a red title 'Resumen' and a bulleted list of four items: 'Problemática', 'Arquitectura', 'Soluciones/Gestión', and 'Preguntas'.

Resumen

- Problemática
- Arquitectura
- Soluciones/Gestión
- Preguntas

Gracias!

Rodrigo Coloritto

Rodrigo.Coloritto@la.logicalis.com



Logicalis llegó a las Redes Sociales

¿Qué esperas para seguirnos?



54

[/LogicalisLatam](#)[@LogicalisLatam](#)[/LogicalisLatam](#)[/Logicalis](#)