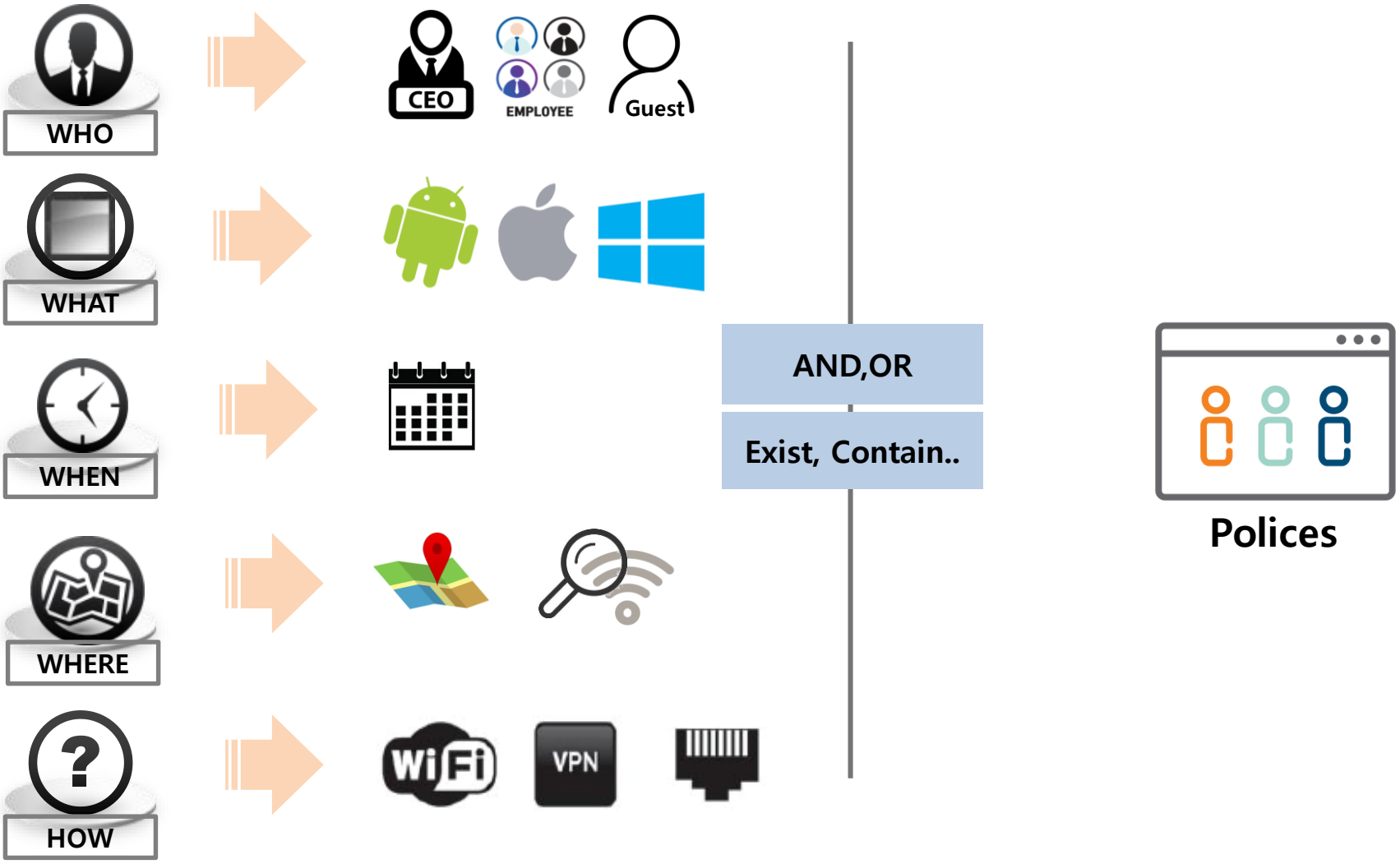
HPe-Aruba ClearPass 구축 사례

UBER SYSTEMS Inc.

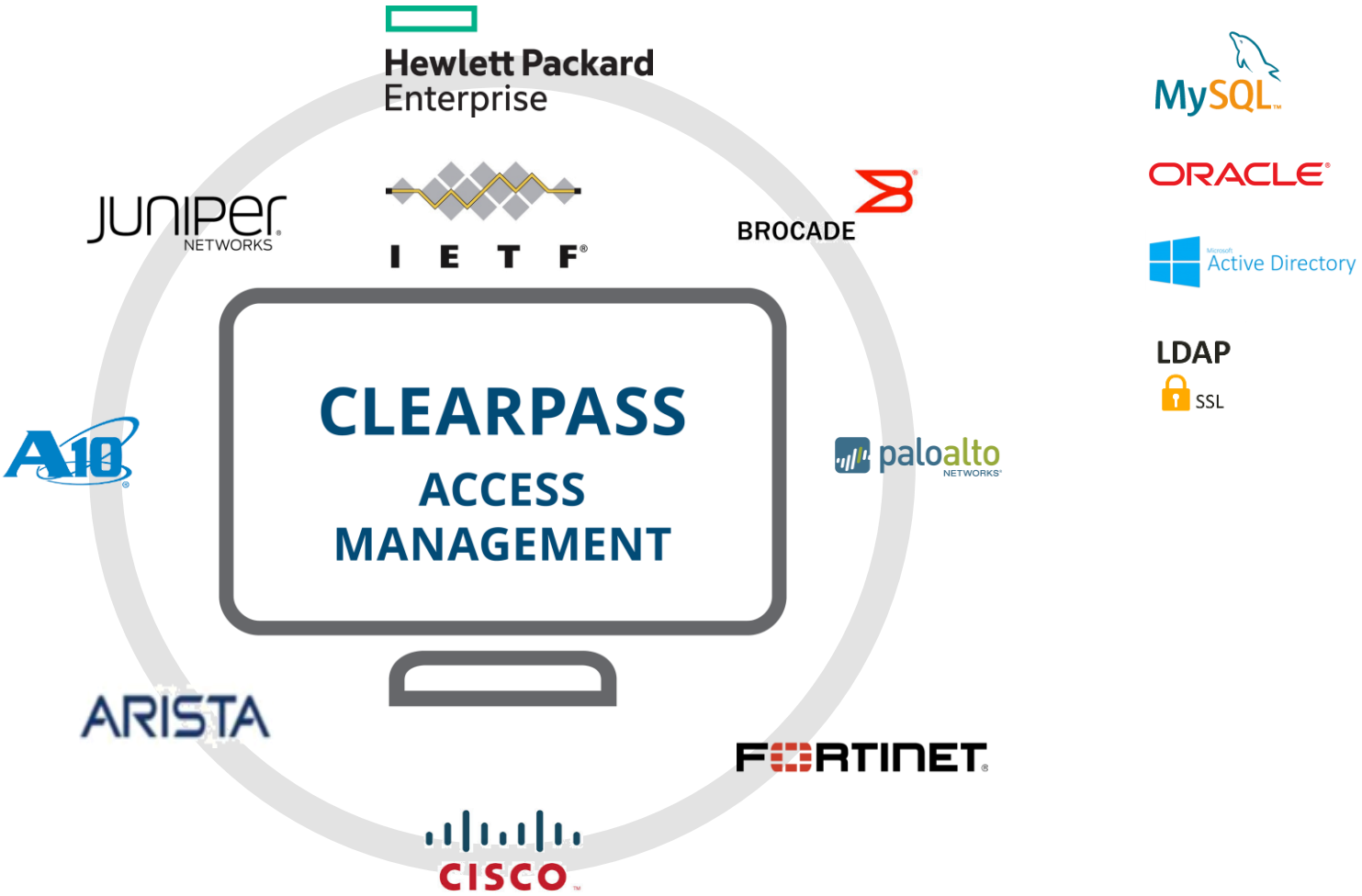
백 인 진 과장

What? Aruba ClearPass

What? Aruba ClearPass



What? Aruba ClearPass



S대학교 아루바 클리어패스 적용 사례

오라클 DB내의 Member 별 SSID 접속 제한

802.1X
무선 접근

ORACLE

CLEARPASS
ACCESS
MANAGEMENT

Publisher

EDU WiFi Guest

S대학교 아루바 클리어패스 적용 사례

UBER SYSTEMS

오라클 DB내의 Member 별 SSID 접속 제한

Configuration

Filter Name: .ORACLE.DB

Login Status:	ACCEPT
Session Identifier:	R003257c2-01-5ca2e46b
Date and Time:	Apr 02, 2019 13:26:19 KST
End-Host Identifier:	BC543
Username:	19049
Access Device IP/Port:	211.252. (CTR1 / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	SMU.WIFI.RADIUS
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	Sql:192.
Authorization Source:	Oracle.11g
Roles:	_WiFi, [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

user_group

Data type

String

Login Status:	ACCEPT
Session Identifier:	R0032584b-01-5ca2e4f0
Date and Time:	Apr 02, 2019 13:28:32 KST
End-Host Identifier:	F4428
Username:	yo
Access Device IP/Port:	211.252. (_CTR1 / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	RADIUS
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	Sql:192
Authorization Source:	Oracle.11g
Roles:	EDU, [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Online

DB내 Member를 ClearPass 사용자 Role에 적용
Role에 따른 정책을 적용하여 서비스 진행

Enforc

Descri

Defaul

Rules

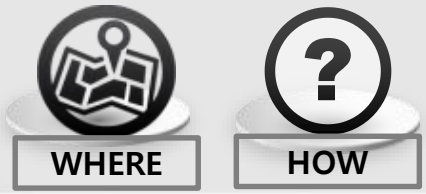
1.	(Tips:Role EQUALS _EDU) AND (Connection:SSID EQUALS Edu)	[Allow Access Profile]
2.	(Tips:Role EQUALS _WiFi) AND (Connection:SSID EQUALS _WiFi)	[Allow Access Profile]
3.	(Tips:Role EQUALS GUEST) AND (Connection:SSID EQUALS _Guest)	[Allow Access Profile]

point

Member별 무선을 통해 접근 통제가 가능하여 보안이 강화.

K사 아루바 클리어패스 적용 사례

층별 분류에 따른 VLAN 할당



K사 아루바 클리어패스 적용 사례

층별 분류에 따른 VLAN 할당

	Conditions	Role
1.	(Connection:AP-Name *CONTAINS* -13F-AP-)	_13F
2.	(Connection:AP-Name *CONTAINS* -14F-AP-)	_14F
3.	(Connection:AP-Name *CONTAINS* -15F-AP-)	_15F

AP Hostname에 층을 입력하여 Role적용 후 Contain 층 Type통한 VLAN 분류

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* _15F)	15F_Dynamic_VLAN_111
2.	(Tips:Role *EQUALS* _14F)	14F_Dynamic_VLAN_112
3.	(Tips:Role *EQUALS* _13F)	13F_Dynamic_VLAN_113

point

1개의 SSID를 통해 특정 층에 VLAN을 할당하여 층에 존재하는 AirPlay 만 확인 가능

- SSID에는 하나의 VLAN이 설정 되여 층상관없이 불필요하게 모든 AirPlay가 확인.

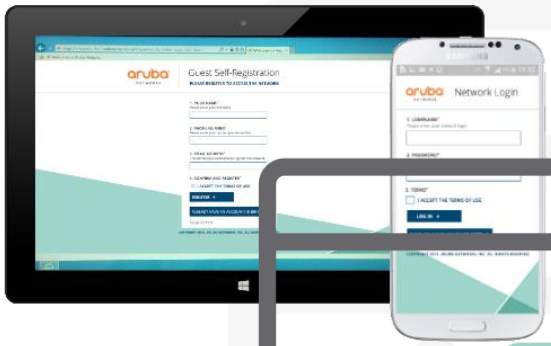
L사 아루바 클리어패스 적용 사례

내방객 Self-registartion을 통한 내방객 전용 SSID 접속

WHO | WHEN | HOW

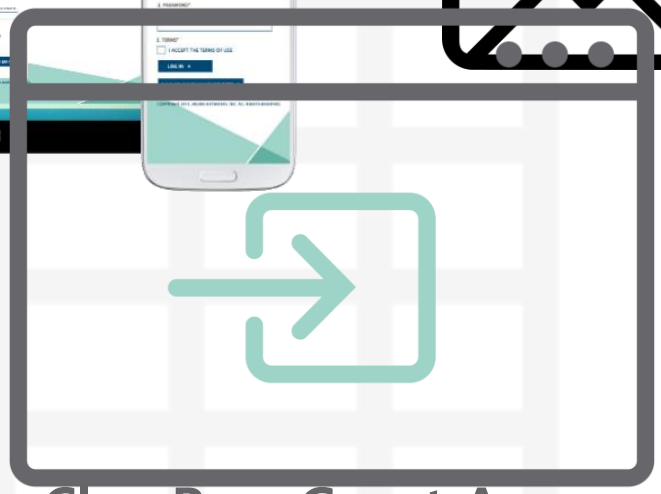
웹 인증 & 계정 생성

가입 승인 요청 메일



내방객 무선 접근

내방객 계정 Expired 1Day



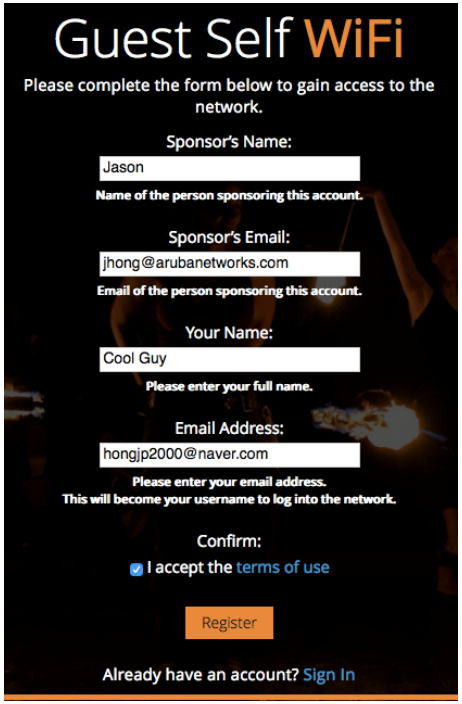
ClearPass Guest Access

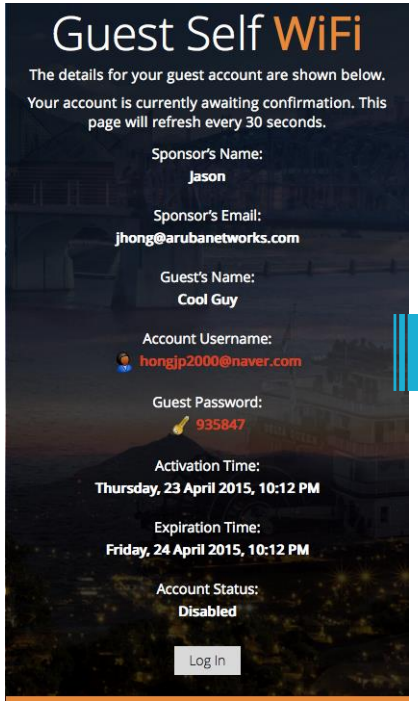
내방객 무선 접근허가

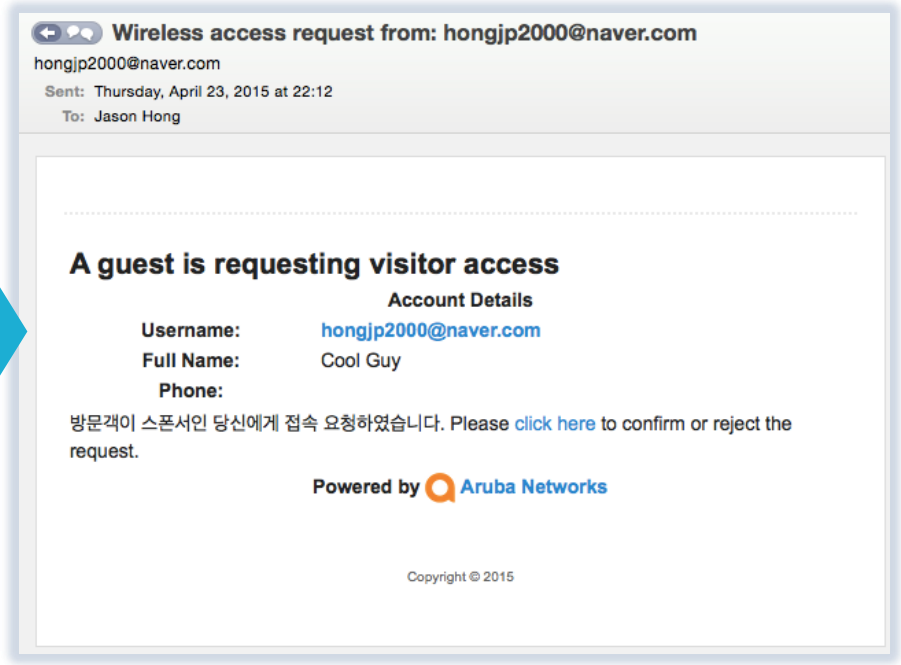
L사 아루바 클리어패스 적용 사례

내방객 Self-registartion을 통한 내방객 전용 SSID 접속

WHO | WHEN | HOW







point

내방객 무선 접근 편의성을 위해 내방객이 직접 계정 생성으로 내방객에 대한 편의성

담당자에게 승인 후 계정을 통한 무선 접근 가능 (무분별한 사용을 막기 위해 Expired 1day적용)

N사 아루바 클리어패스 적용 사례

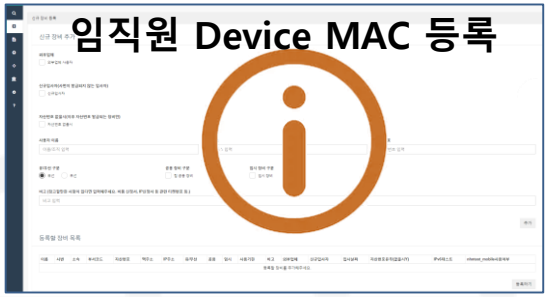
UBER SYSTEMS

임직원 유무선 사용자 Role에 따른 VLAN 할당

WHO

HOW

REST API



REST API

유무선 접근
MAC인증 접근제어

CLEARPASS
ACCESS
MANAGEMENT

Publisher Sync Subscriber

접근 허가
Dynamic VLAN정책 부여

N사 아루바 클리어패스 적용 사례

임직원 유무선 사용자 Role에 따른 VLAN 할당

User ID:	AA:BB:CC:DD:EE:FF
Name:	Ubersystems
Password:	••••••••••••••
Verify Password:	••••••••••••••
Enable User:	(Check to enable user)
Change Password:	(Check to force change password on next TACACS+ login)
Role:	v561

Configuration » Services » Edit - [NHNENT_MAC_AUTH]

Services - [NHNENT_MAC_AUTH]

Summary | Service | Authentication | Authorization | Roles | Enforcement

Use Cached Results:	Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	MAC_Dynamic_VLAN Modify Add new Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS v561)	_V561
2.	(Tips:Role EQUALS v562)	_V562
3.	(Tips:Role EQUALS v563)	_V563
4.	(Tips:Role EQUALS v564)	_V564
5.	(Tips:Role EQUALS v565)	_V565
6.	(Tips:Role EQUALS v566)	_V566
7.	(Tips:Role EQUALS v567)	_V567
8.	(Tips:Role EQUALS v568)	_V568
9.	(Tips:Role EQUALS v311)	_V311
10.	(Tips:Role EQUALS v421)	_V421
11.	(Tips:Role EQUALS v431)	_V431

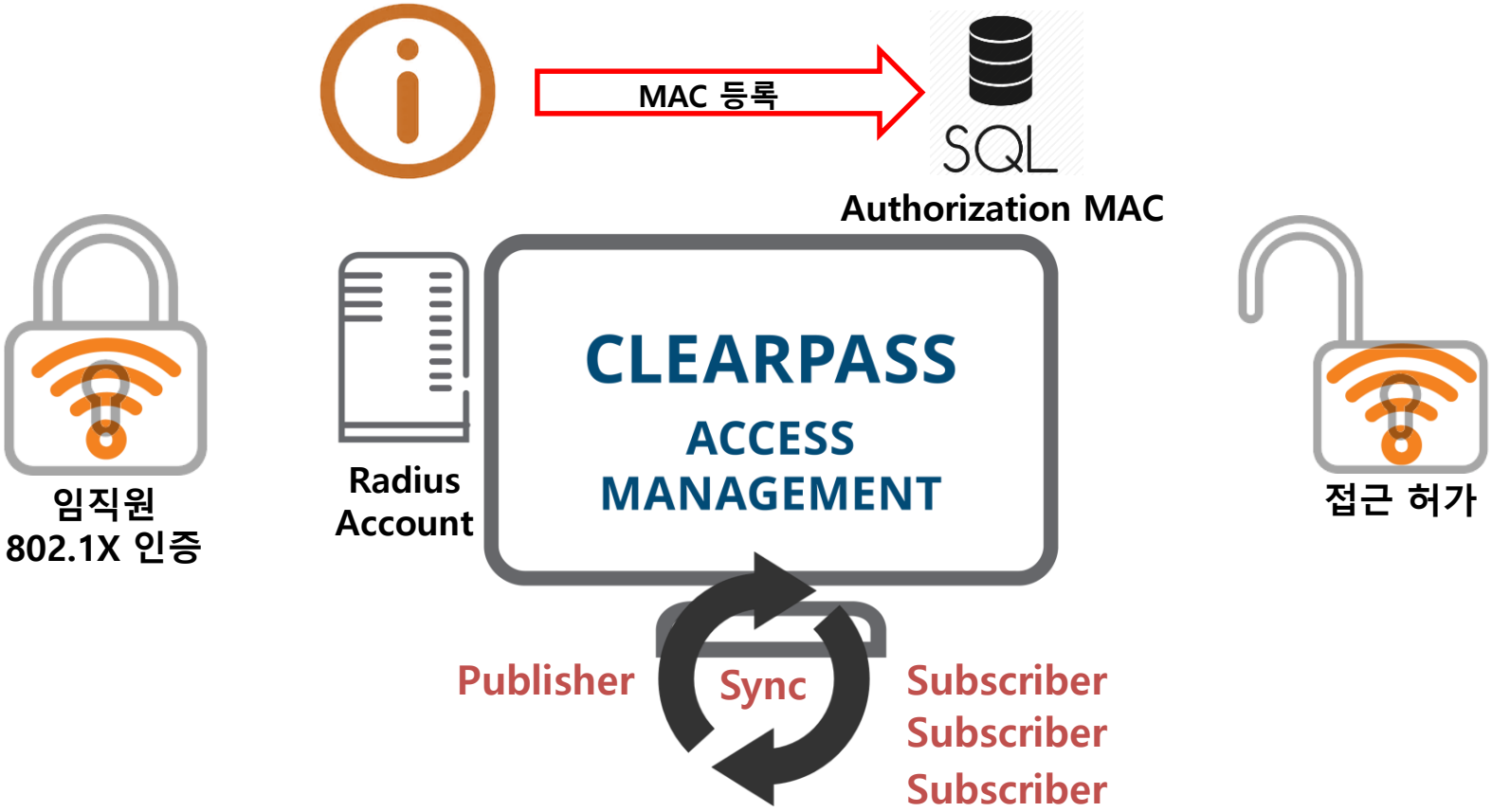
Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	108800
2.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)
3.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
4.	Radius:IETF	Tunnel-Type	=	VLAN (13)
5.	Radius:IETF	Tunnel-Private-Group-Id	=	561

point 임직원 VLAN Role에 따른 VLAN 할당하여 임직원의 대역 관리의 편의성.

N사 아루바 클리어패스 적용 사례

임직원 무선 사용자 MAC등록 후 VLAN할당



N사 아루바 클리어패스 적용 사례

임직원 무선 사용자 MAC등록 후 VLAN할당

	Conditions	Role
1.	(Authorization:MySQL_DB(10.114.27.251):mac *EXISTS*)	[Employee]
2.	(Authorization:MySQL_DB(10.114.27.251):mac *NOT_EXISTS*)	[Guest]

SQL DB에 MAC이 존재 할 경우 Employee Role을 부여
Role에 따라 VLAN 할당

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* [Guest])	VLAN111, mac-redirect
2.	(Tips:Role *EQUALS* [Employee])	[Update Endpoint Known], [Allow Access Profile]

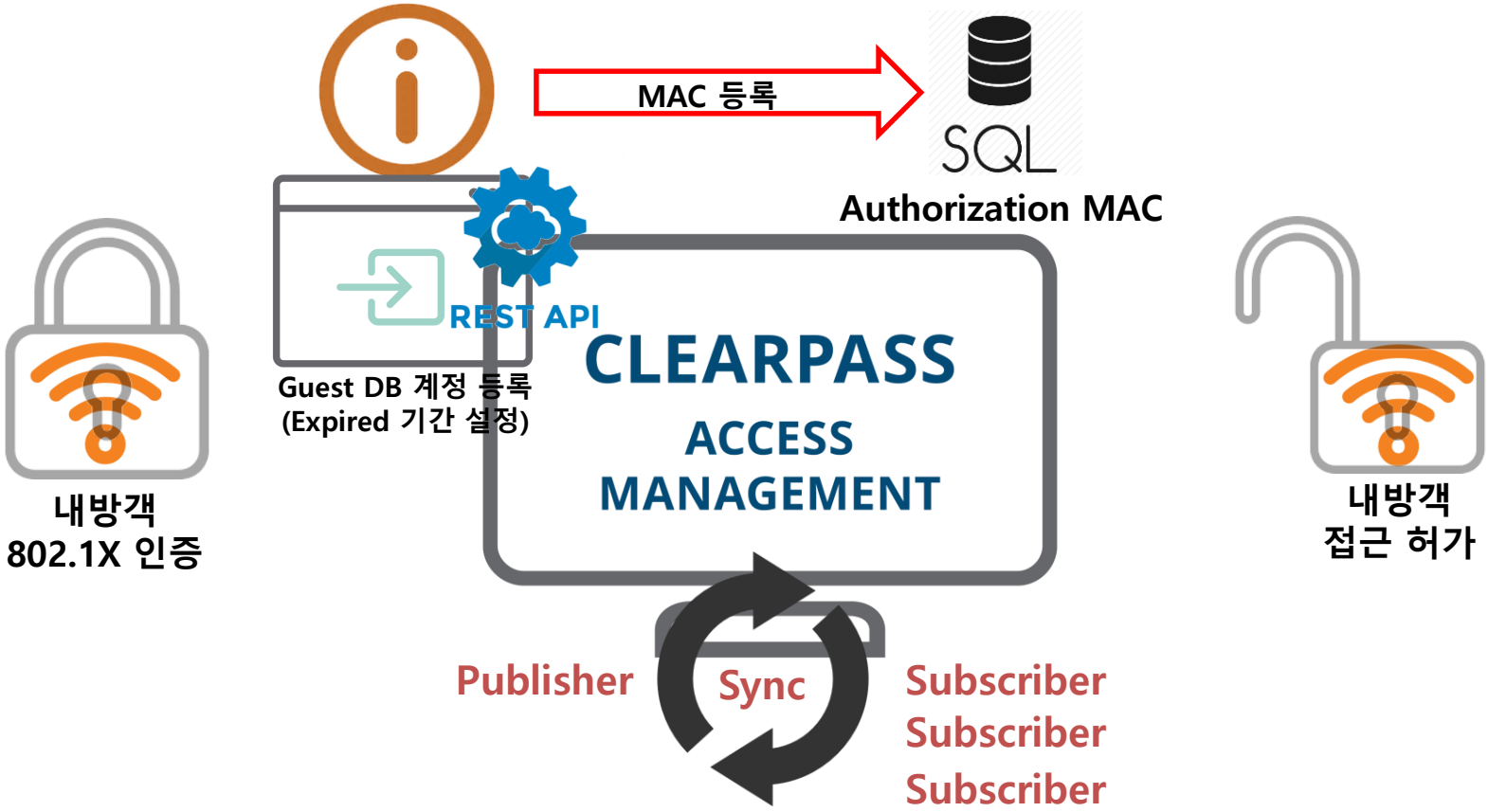
point

사용자 MAC이 존재 할 경우 인증 적용으로 보다 무선 접속에 대한 보안 강화

Guest Role일 경우 Mac 등록 안내 페이지로 Redirect 진행으로 관리 편의성

N사 아루바 클리어패스 적용 사례

내방객 무선 사용자 서비스 적용



N사 아루바 클리어패스 적용 사례

UBER SYSTEMS

내방객 무선 사용자 서비스 적용

REST API

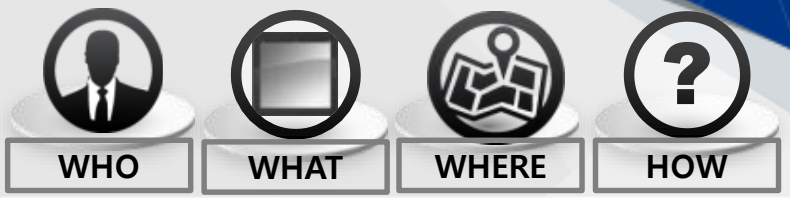
00270629	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
15497999	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
30401153	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
40080591	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
45296276	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
60349944	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
70642056	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
71314959	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
82592597	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
89695092	[Guest]	Active	2017-05-04 17:31	No expiry	해당없음
aaun3657	[Guest]	Pending	In 11.4 일	2019-04-27 01:59	해당없음
aepu0913	[Guest]	Active	2019-01-07 00:00	2019-04-07 23:59	해당없음
afip4632	[Guest]	Active	24.7 일 ago	2019-05-31 23:59	해당없음
aggl0877	[Guest]	Pending	In 74분	2019-03-28 22:00	해당없음
agtf9400	[Guest]	Active	22.6 일 ago	2019-06-05 01:59	해당없음

point

내방객 계정은 Restful API를 통해 Guest DB에 등록으로 내방객 관리 용이

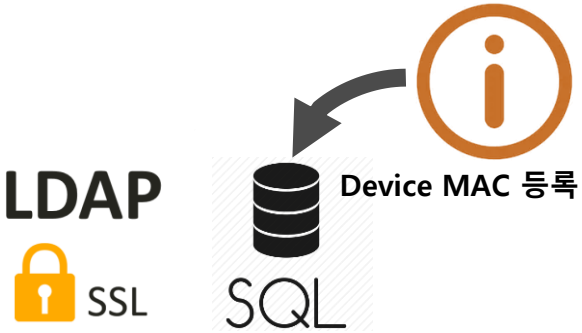
K사 아루바 클리어패스 적용 사례

유무선 & Device 인증 진행



MAC 인증

MAC Vendor
MAC OUI
MAC Address

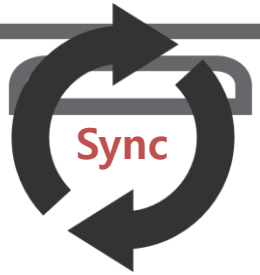


CLEARPASS
ACCESS
MANAGEMENT

802.1X 인증

MAC Address
여부에 따른 등급 분류

유무선 접근

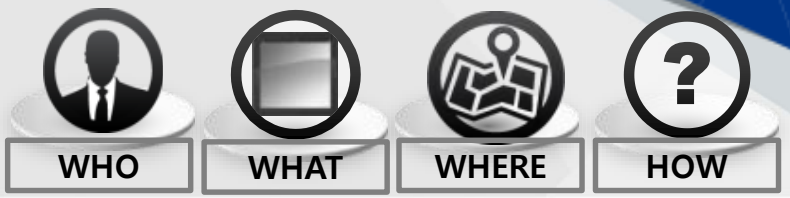


접근 허가
정책에 따른 VLAN 할당

K사 아루바 클리어패스 적용 사례

UBER SYSTEMS

유무선 & Device 인증 진행



IP PHONE

Filter: Name contains Go Clear Filter Show 20 records

#		Order	Name	Type	Template	Status
1.		1	00.IPT	RADIUS	MAC Authentication	

클리어패스의 서비스는 정책에 부합해야 적용 되며, IP PHONE 같은 경우 Vendor & MAC 정보 등록으로 인해 서비스 부합

	Type			Value	
1.	Connection	Client-Mac-Vendor	CONTAINS	M	E
2.	Connection	Client-Mac-Address	BEGINS_WITH	18:	
3.	Connection	Client-Mac-Address	BEGINS_WITH	00:	
4.	Connection	Client-Mac-Address	BEGINS_WITH	f4:	
5.	Connection	Client-Mac-Address	BEGINS_WITH	F4:	
6.	Connection	Client-Mac-Address	EQUALS	00:	64
7.	Connection	Client-Mac-Address	EQUALS	00:	67
8.	Connection	Client-Mac-Address	BEGINS_WITH	20:	
9.	Connection	Client-Mac-Address	BEGINS_WITH	00:	
10.	Connection	Client-Mac-Address	BEGINS_WITH	a8:	
11.	Connection	Client-Mac-Address	EQUALS	00:	

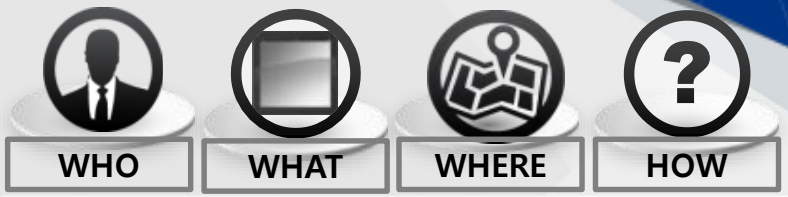
point

IP Phone 경우 Vendor & MAC-Address 정보를 통해 서비스를 이용

- 유선 스위치의 특정 설정 없이 정책에 따른 VLAN할당으로 편리성 용이

K사 아루바 클리어패스 적용 사례

유무선 & Device 인증 진행



유무선 Authentication

Role Mapping Policy Details	
Description:	MAC 등록 판별
Default Role:	[Guest]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Role
1.	(Authorization: _MAC_DB:macaddr *EXISTS*)	[Employee]
2.	(Authorization: _MAC_DB:macaddr *EXISTS*)	[Employee]
3.	(Authorization: _MAC_DB:macaddr *NOT_EXISTS*) *OR* (Authorization: _MAC_DB:macaddr *NOT_EXISTS*)	[Guest]

SQL DB에 사용자 MAC의 존재여부 (EXISTS & NOT_EXISTS)에 따라 Role 부여

point

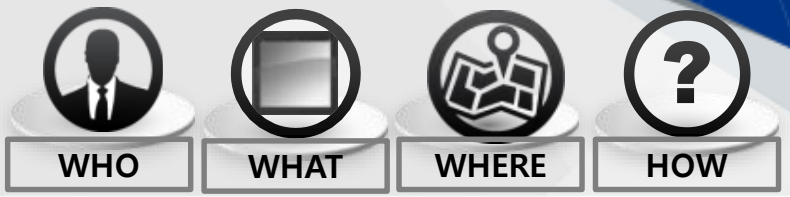
SQL DB의 정보를 Query하여 MAC의 존재여부를 확인

- 존재 여부 확인에 따라 구성 된 Role을 할당.

K사 아루바 클리어패스 적용 사례

UBER SYSTEMS

유무선 & Device 인증 진행



유무선 Authentication

Description:	& MAC auth		
Default Profile:	0. _profiled_test02		해당 정책에 속하지 않을 시 Default profile 정책을 적용.
Rules Evaluation Algorithm:	first-applicable		
	Conditions	**Enforcement Profiles**	
1.	(Authorization: _LDAP:deptNamePath EQUALS 채널;인프라 ;협력사;)	[Deny Access Profile]	특정 그룹은 REJECT (자회사 또는 협력사 일 경우) 별도 서비스를 부여
2.	(Authorization: _LDAP:deptNamePath EQUALS [채널];인프라 ;협력사;)	[Deny Access Profile]	
3.	(Connection:Client-Mac-Address EQUALS 00: :f:0c)	0. wired_kown_windows, username	특정 MAC
4.	(Connection:Client-Mac-Address EQUALS 50: BE:07)	0. wired_security_vlan323, username	
5.	(Connection:Client-Mac-Address EQUALS A0: E0:15)	username, ecurity_vlan323	
6.	(Connection:Client-Mac-Address EQUALS 50: 3:9d)	username, ecurity_vlan323	
7.	(Connection:Client-Mac-Address EQUALS C4: 5D:31)	username, ecurity_vlan323	
8.	(Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization: _LDAP:deptNamePath CONTAINS 컴퍼니;; 머스;)	username, _Wired_PC_VLAN_903	Device Type & 특정그룹
9.	(Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization: _LDAP:deptNamePath CONTAINS 컴퍼니)	username, _pc_vlan622	
10.	(Tips:Role EQUALS [Employee]) AND (Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization: MAC_DB:authtype EQUALS 1) AND (Authorization: LDAP:deptNamePath CONTAINS ;CTO;인프라 ;인프라 1팀;정보보안파트;)	username, ecurity_vlan323	Role & Device Type & 특정 그룹
11.	(Tips:Role EQUALS [Employee]) AND (Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization: _MAC_DB:authtype EQUALS 1) AND (Authorization: _LDAP:deptNamePath CONTAINS ;CTO;인프라 실;인프라 2팀;)	username, _infra_vlan324	
12.	(Tips:Role EQUALS [Employee]) AND (Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization: _MAC_DB:authtype EQUALS 1) AND (Authorization: LDAP:deptNamePath CONTAINS ;CTO;인프라 ;인프라 1팀;클라우드컴퓨팅파트)	username, _infra_vlan324	
13.	(Tips:Role EQUALS [Employee]) AND (Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization:1 _MAC_DB:authtype EQUALS 1) AND (Authorization: _LDAP:deptNamePath CONTAINS ;CTO;인프라플랫폼실;인프라	username, dbpart_vlan325	

point

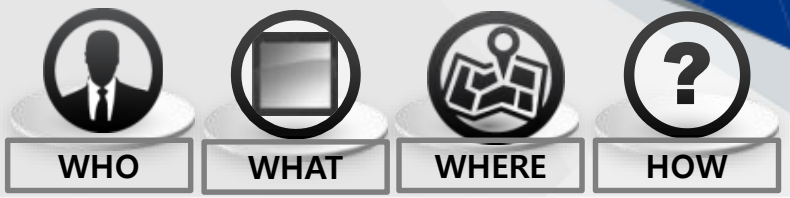
특정 그룹 & Role & Device Type & LDAP 그룹에 따른 정책 적용

- AND 조건을 통한 정책에 따라 VLAN 할당.

K사 아루바 클리어패스 적용 사례

UBER SYSTEMS

유무선 & Device 인증 진행



유무선 Authentication

21.	(Tips:Role EQUALS [Employee]) AND (Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization:[Endpoints Repository]:OS Family NOT_EQUALS Windows) AND (Authorization: _MAC_DB:authtype EQUALS 1) AND (Authorization: _LDAP:employeeNumber ENDS_WITH 7)	0. wired_nonwindows_vlan322, username
22.	(Tips:Role EQUAL AND (Authoriza AND (Authoriza AND (Authoriza	
23.	(Tips:Role EQUAL AND (Authoriza AND (Authoriza AND (Authoriza	
24.	(Tips:Role EQUAL AND (Authoriza AND (Authoriza AND (Authoriza	ce Type & OS에 정책 적용
25.	(Tips:Role EQUAL AND (Authoriza AND (Authoriza AND (Authoriza	
26.	(Tips:Role EQUAL AND (Authoriza AND (Authoriza AND (Authoriza	
27.	(Tips:Role EQUAL AND (Authoriza AND (Authoriza AND (Authorization:[Endpoints Repository]:Status EQUALS Known)	
28.	(Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Windows) AND (Authorization:[Endpoints Repository]:Status EQUALS Unknown)	y Access Profile]
29.	(Authorization:0.KAKAO_LDAP:deptNamePath CONTAINS 카카오 패밀리컴퍼니;)	0. wired_non_profiled
30.	(Tips:Role EQUALS [Guest])	01.Unknow_MAC_Wired_VLAN_900

해당 단말은 MAC Address 관리 시스템에 등록이 안되어
사내 네트워크 사용이 불가합니다.
아래 url에서 본인의 단말 MAC Address 등록이 되어있는지 확인후
아래 담당자에게 문의하시기 바랍니다.

총무자산-내자산보기

point

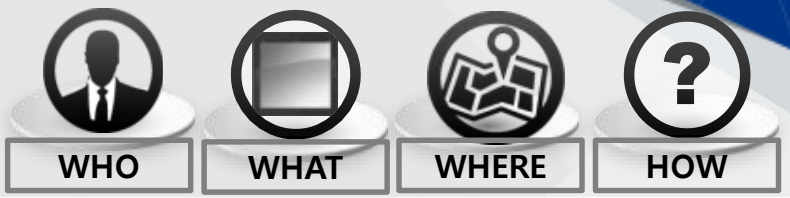
Guest경우 안내 페이지로 Redirect Role 적용.

- Guest는 모든 정책이 부합하지 않아 서비스 접근을 막지만 사유를 확인 하기 위한 안내페이지 Redirect

K사 아루바 클리어패스 적용 사례

UBER SYSTEMS

유무선 & Device 인증 진행



유무선 Authentication (자회사)

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	1 Wireless_Policy Modify

Enforcement Policy Details

Description:	Wireless Policy
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* [Employee]) *AND* (Authorization: _MAC_DB:devicetype *EQUALS* APPLE TV)	1.Family_OA_ETC_VLAN_701
2.	(Tips:Role *EQUALS* [Employee]) *AND* (Authorization: _MAC_DB:devicetype *EQUALS* IOT) *AND* (Authorization: _MAC_DB:authtype *EQUALS* 2)	1.Family_IOT_VLAN_702
3.	(Tips:Role *EQUALS* [Employee]) *AND* (Authorization: _MAC_DB:devicetype *EQUALS* IOT) *AND* (Authorization: _MAC_DB:authtype *EQUALS* 1)	1.Family_IOT_VLAN_601
4.	(Tips:Role *EQUALS* [Employee]) *AND* (Authorization:1 MAC_DB:devicetype *EQUALS* PC) *AND* (Authorization:1 MAC_DB:authtype *EQUALS* 1) *AND* (Authorization:0 _LDAP:deptNamePath *CONTAINS* 리컴퍼니;)	1.Family_WLAN_PC_VLAN_401
5.	(Tips:Role *EQUALS* [Employee]) *AND* (Authorization:1 MAC_DB:devicetype *CONTAINS* MOBILE) *AND* (Authorization:1 MAC_DB:authtype *EQUALS* 1) *AND* (Authorization:0 _LDAP:deptNamePath *CONTAINS* 리컴퍼니;)	1.Family_WLAN_Mobile_VLAN_501


Thank you