Windows 7 인증접속 메뉴얼

정보통신팀 2012.08

Wireless LAN 설정

WZC 설정 전 무선 랜카드 및 서비스가 정상적으로 동작 중인지 확인합니다.

1. 네트워크 및 인터넷 설정

2. 무선 네트워크 관리



시작→제어판 → 네트워크 및 인터넷 → 네트워크 및 공유센터 → 무선 네트워크 관리



3. 무선 네트워크 연결을 사용하는 무선 네트워크 관리



추가 →네트워크 추가

4. 추가할 무선 네트워크에 대한 정보를 입력

우가일 구선 네	-워크에 대한 경도를 합덕아접시도	2.
네트워크 이름(E):	Welcome_KAIST	
보안 종류(<u>S</u>):	2WPA2-엔터프라이즈 ▼	
암호화 유형(<u>R</u>):	3 AES	
보안 키(<u>C</u>):] 문자 숨기기(<u>H</u>)
④ 자동으로 이 연	결 시작(I)	
🔲 네트워크에서	브로드캐스팅하지 않는 경우에도 연결(Q)	
경고: 이 옵션을	을 선택하면 사용자 개인 정보 보호에 위험이 미	마를 수 있습니다.

- 1. 네트워크 이름 : Welcome_KAIST
- 2. 보안 종류 : WPA2-엔터프라이즈
- 3. 암호화 유형 : AES
- 4. 자동으로 이 연결 시작 : 사용자 선택 사항
- 5. 다음 클릭 →연결 설정 변경 클릭



5. 무선 네트워크 연결을 사용하는 무선 네트워크 관리

Welcome_KAIST 무선 네트워크 속성 연결
보안 종류(E): 2 WPA2-엔터프라이즈 암호화 유형(Ŋ): 3 AES
④ 네트워크 인증 방법 선택(<u>0</u>): ④ Microsoft: PEAP(Protected Extensible A 설정(<u>S</u>) ▼ 로그온할 때마다 이 연결에 사용되는 내 자격 증명 기억(<u>B</u>)
고급 설정(D)
<u>확인</u> 취소

- 1. 보안 탭을 이동
- 2. 보안 종류 : WPA2-엔터프라이즈
- 3. 암호화 유형 : AES
- 4. 네트워크 인증 방법 선택 : Microsoft: 보호된 EAP(PEAP)
- 5. 확인 버튼을 누르기 전에 설정 버튼 클릭

6. 보호된 EAP 속성

보호된 EAP 속성
1 - [서비 인증서 유효성 확인(V)] -] 다음 서비에 연결(<u>O</u>):
신뢰할 수 있는 루트 인증 기관(<u>B</u>):
Class 3 Public Primary Certification Authority Equifax Secure Certificate Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Timestamping CA
교재 서비 또는 인상 기관을 허가하도록 사용자에게 듣지 않음(만) 2 민증 방법 선택(<u>S</u>):
보안된 암호(EAP-MSCHAP v2)
확인 취소

- 1. 연결할 때 : 서버 인증서 유효성 확인 체크 해제
- 2. 인증 방법 선택 : 보안된 암호(EAP-MSCHAP v2) 선택
- 3. 확인 버튼을 누르기 전에 구성 버튼 클릭



7. EAP MSCHAPv2 속성

EAP MSCHAPv2 속성
연결할 때:
① 사동음로 Windows 로그온 이름 및 암호(도메인이)
확인 취소

자동으로 Windows 로그온 이름 및 암호 사용 체크 해제
 확인

8. 보호된 EAP 속성 확인

보호된 EAP 속성
연결할 때 : 전
신뢰할 수 있는 루트 인증 기관(<u>B</u>):
Class 3 Public Primary Certification Authority Equifax Secure Certificate Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Premium Server CA Thawte Timestamping CA
□ 새 서버 또는 인증 기관을 허가하도록 사용자에게 묻지 않음(₽)
인증 방법 선택(<u>S</u>): 보안된 암호(EAP-MSCHAP v2)
 ✓ 빠른 다시 연결 사용(E) □ 네트워크 액세스 보호 적용(N) □ 서버에 Cryptobinding TLV가 없으면 연결 끊기(D) □ ID 프라미버시 사용(I)

1. 확인



9. 고급 설정(선택사항)

연결 보안			
보안 종류(E): 암호화 유형(N	(WPA2- AES	엔터프라이즈	•
네트워크 인증 Microsoft: PE V 로그온할 따	방법 선택(0): AP(Protected E: I마다 이 연결에 ,	ktensible A ▾) 사용되는 내 자격 중	설정(S) 명 기억(R)
1 고급 설2	령(D)		

1. 고급 설정 선택

10.802.1X 설정(선택사항)



- 1. 인증 모드 지정 체크
- 2. 사용자 인증 선택
- 3. 자격 증명 저장 클릭



11. 자격 증명 저장(선택사항)

고급 설정	War war and the	Σ
802,1X 설정	802,11 설정	
	코드 지정(P):	-
Vindows 보안		×
자격 증명 자격 증명을 7 다(예: 업데이:	저장 讨장하면 로그온하지 않고도 네트워크에 연결할 수 있습니 트를 다운로드하는 경우).	
	(1) [사용자 이름 [암호	
	확인 취소	
	(\$10) (\$1 A	
	목인 위오	

- 사용자 계정을 저장(선택)
 자격 증명 저장에 계정을 저장하면 무선랜 접속시 자동 로그인



12. 프로필 유형(선택사항)



13. 802.1X 설정(선택사항)



- 1. 생성된 프로파일을 선택하고
- 2. 프로필 유형 클릭



14. 추가된 프로파일 확인 및 무선랜 연결



1. 화면 오른쪽 하단의 무선랜 표시를 클릭

15. Welcome_KAIST 연결

연결되어 있지 않음 😚		
무선 네트워크 연결 🔹		
Welcome_KAIST		
	연결(<u>C</u>)	
ITDEV2	이름: Welcome_KAIST	
ITDEV1	신호 경도, 매우 경험 보안 종류: WPA2 리티아 조류: 902 11a	
IPv4_KAIST	SSID: Welcome_KAIST	
ollehEgg_034	att	
Hwangs	.atl	
기타 네트워크	- III-	
네트워크 및 공유 센터 열기		

1. Welcome_KAIST 클릭 → 연결 버튼 클릭