# ACS 5.1 및 Windows 2003 Server가 있는 UWN에서 PEAP

## 목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기규칙 구성 네트워크 다이어그램 IIS, 인증 기관, DNS, DHCP(CA)를 사용한 Windows Enterprise 2003 설치 CA(데모카) Cisco 1121 Secure ACS 5.1 <u>CSACS-1121 Series Appliance를 사용한 설치</u> ACS 서버 설치 Cisco WLC5508 컨트롤러 컨피그레이션 WPAv2/WPA에 필요한 구성을 만듭니다. PEAP 인증 인증서 템플릿 스냅인 설치 ACS 웹 서버용 인증서 템플릿 만들기 새 ACS 웹 서버 인증서 템플릿 활성화 ACS 5.1 인증서 설정 ACS용 내보내기 가능 인증서 구성 ACS 5.1 소프트웨어에 인증서 설치 <u>Active Directory에 대한 ACS ID 저장소 구성</u> ACS에 AAA 클라이언트로 컨트롤러 추가 무선에 대한 ACS 액세스 정책 구성 ACS 액세스 정책 및 서비스 규칙 생성 Windows Zero Touch를 사용하는 PEAP에 대한 클라이언트 구성 기본 설치 및 구성 수행 무선 네트워크 어댑터 설치 무선 네트워크 연결 구성 ACS로 무선 인증 문제 해결 ACS 서버에서 PEAP 인증 실패 관련 정보

## <u>소개</u>

하여 PEAP(Protected Extensible Authentication Protocol)를 통해 Wireless LAN Controller, Microsoft Windows 2003 소프트웨어 및 Cisco ACS(Secure Access Control Server) 5.1을 사용하여 보안 무선 액세스를 구성하는 방법에 대해 설명합니다.

**참고:** 보안 무선 구축에 대한 자세한 내용은 <u>Microsoft Wi-Fi 웹 사이트</u> 및 <u>Cisco SAFE 무선 청사진</u> <u>을 참조하십시오</u>.

## <u>사전 요구 사항</u>

## <u>요구 사항</u>

이 문서에서는 테스트를 쉽게 수행할 수 있도록 특정 컨피그레이션만 다루므로 설치 프로그램에서 기본 Windows 2003 설치 및 Cisco Wireless LAN Controller 설치에 대해 알고 있다고 가정합니다.

Cisco 5508 Series Controller의 초기 설치 및 컨피그레이션 정보는 <u>Cisco 5500 Series Wireless</u> <u>Controller 설치 설명서를 참조하십시오</u>. Cisco 2100 Series Controller의 초기 설치 및 컨피그레이션 정보는 <u>Quick Start Guide: Cisco 2100 Series Wireless LAN Controller를 참조하십시오</u>.

Microsoft Windows 2003 설치 및 구성 가이드는 <u>Windows Server 2003 R2 설치에서 찾을</u> 수 있습 니다.

시작하기 전에 테스트 랩의 각 서버에 Microsoft Windows Server 2003 SP1 운영 체제를 설치하고 모든 서비스 팩을 업데이트하십시오. 컨트롤러 및 LAP(Lightweight Access Point)를 설치하고 최신 소프트웨어 업데이트가 구성되었는지 확인합니다.

Windows Server 2003 SP1, Enterprise Edition은 PEAP 인증을 위한 사용자 및 워크스테이션 인증 서의 자동 등록을 구성할 수 있도록 사용됩니다. 인증서 자동 등록 및 자동 갱신을 통해 인증서를 더 쉽게 구축하고 인증서를 자동으로 만료 및 갱신하여 보안을 강화할 수 있습니다.

### <u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 7.0.98.0을 실행하는 Cisco 2106 또는 5508 Series 컨트롤러
- Cisco 1142 LWAPP(Lightweight Access Point Protocol) AP
- IIS(Internet Information Server), CA(Certificate Authority), DHCP 및 DNS(Domain Name System)가 설치된 Windows 2003 Enterprise
- Cisco 1121 Secure ACS(Access Control System Appliance) 5.1
- Windows XP Professional(SP 및 업데이트된 서비스 팩) 및 무선 NIC(네트워크 인터페이스 카 드)(CCX v3 지원) 또는 타사 신청자
- Cisco 3750 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### <u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

## <u>구성</u>

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** 이 섹션에 사용된 <u>명령에</u> 대한 자세한 내용을 보려면<u>명령</u> 조회<u>도구(</u>등록된 고객만 해당)를 사용하십시오.

### <u>네트워크 다이어그램</u>

이 문서에서는 이 네트워크 설정을 사용합니다.

Cisco Secure Wireless Lab 토폴로지



이 문서의 주 목적은 ACS 5.1 및 Windows 2003 Enterprise Server가 있는 Unified Wireless Networks에서 PEAP를 구현하기 위한 단계별 절차를 제공하는 것입니다. 클라이언트가 자동으로 등록하고 서버에서 인증서를 가져오도록 클라이언트의 자동 등록에 주안점을 두고 있습니다.

**참고:** Windows XP Professional with SP에 TKIP(Temporal Key Integrity Protocol)/AES(Advanced Encryption Standard)를 사용하는 WPA(Wi-Fi Protected Access)/WPA2<u>를</u> 추가하려면 <u>Windows</u> <u>XP 서비스 팩 2의 WPA2/WPS IE(Wireless Provisioning Services Information Element) 업데이트를</u> 참조하십시오.

## <u>IIS, 인증 기관, DNS, DHCP(CA)를 사용한 Windows Enterprise</u> 2003 설치

### <u>CA(데모카)</u>

CA는 Windows Server 2003 SP2, Enterprise Edition을 실행하는 컴퓨터로, 다음 역할을 수행합니

다.

- IIS를 실행하는 demo.local 도메인의 도메인 컨트롤러입니다
- demo.local DNS 도메인용 DNS 서버
- DHCP 서버
- demo.local 도메인에 대한 엔터프라이즈 루트 CA

이러한 서비스에 대해 CA를 구성하려면 다음 단계를 수행합니다.

- 1. <u>기본 설치 및 구성을 수행합니다.</u>
- 2. <u>컴퓨터를 도메인 컨트롤러로 구성합니다.</u>
- 3. <u>도메인 기능 수준을 올립니다.</u>
- 4. <u>DHCP를 설치하고 구성합니다.</u>
- 5. <u>인증서 서비스를 설치합니다.</u>
- 6. <u>인증서에 대한 관리자 권한을 확인합니다.</u>
- 7. <u>도메인에 컴퓨터를 추가합니다.</u>
- 8. <u>컴퓨터에 대한 무선 액세스를 허용합니다.</u>
- 9. <u>도메인에 사용자를 추가합니다.</u>
- 10. <u>사용자에 대한 무선 액세스를 허용합니다.</u>
- 11. <u>도메인에 그룹을 추가합니다.</u>
- 12. wirelessusers 그룹에 사용자를 추가합니다.
- 13. <u>무선 사용자 그룹에 클라이언트 컴퓨터를 추가합니다.</u>

#### <u>기본 설치 및 구성 수행</u>

다음 단계를 수행합니다.

- 1. Windows Server 2003 SP2, Enterprise Edition을 독립 실행형 서버로 설치합니다.
- 2. IP 주소 10.0.10.10과 서브넷 마스크 255.255.255.0으로 TCP/IP 프로토콜을 구성합니다.

#### <u>컴퓨터를 도메인 컨트롤러로 구성</u>

- 1. Active Directory 설치 마법사를 시작하려면 **시작 > 실행** 을 선택하고 dcpromo.exe를 **입력한 다음 확인** 을 클릭합니다.
- 2. Active Directory 설치 마법사 시작 페이지에서 다음 을 클릭합니다.
- 3. Operating System Compatibility(운영 체제 호환성) 페이지에서 Next(다음)를 클릭합니다.
- 4. Domain Controller Type(도메인 컨트롤러 유형) 페이지에서 **새 도메인에 대한 Domain** Controller(도메인 컨트롤러)를 선택하고 Next(다음)를 클릭합니다.
- 5. Create New Domain(새 도메인 생성) 페이지에서 Domain in a new forest(새 포리스트에서 도 메인)를 선택하고 Next(다음)를 클릭합니다.
- 6. Install or Configure DNS(DNS 설치 또는 구성) 페이지에서 **No(아니요), just install and** configure DNS on this computer(이 컴퓨터에 DNS만 설치 및 구성)를 선택하고 Next(다음)를 클릭합니다.
- 7. New Domain Name(새 도메인 이름) 페이지에서 **demo.local을** 입력하고 **Next(다음**)를 클릭합 니다.
- 8. NetBIOS Domain Name(NetBIOS 도메인 이름) 페이지에서 Domain NetBIOS name as demo(도메인 NetBIOS 이름)를 입력하고 Next(다음)를 클릭합니다.

9. [데이터베이스 및 로그 폴더 위치] 페이지에서 기본 [데이터베이스 및 로그 폴더] 디렉토리를 적용하고 다음을 **누릅니다** 

| Active Directory Installation Wizard  | × |  |  |  |  |
|---|---|--|--|--|--|
| Database and Log Folders<br>Specify the folders to contain the Active Directory database and log files. |   |  |  |  |  |
| For best performance and recoverability, store the database and the log on separate<br>hard disks.      |   |  |  |  |  |
| Where do you want to store the Active Directory database?   |   |  |  |  |  |
| Database folder:  |   |  |  |  |  |
| C:\WINDOWS\NTDS Bjowse  |   |  |  |  |  |
| Where do you want to store the Active Directory log?  |   |  |  |  |  |
| C:\wINDOWS\NTDS Bigwse  |   |  |  |  |  |
|   |   |  |  |  |  |
| < <u>B</u> ack <u>N</u> ext> Cancel   |   |  |  |  |  |

10. Shared System Volume(공유 시스템 볼륨) 페이지에서 기본 폴더 위치가 올바른지 확인하고 Next(**다음**)를 클릭합니다

| Active Directory Installation Wizard  |
|---|
| Shared System Volume<br>Specify the folder to be shared as the system volume.   |
| The SYSVOL folder stores the server's copy of the domain's public files. The contents<br>of the SYSVOL folder are replicated to all domain controllers in the domain. |
| The SYSVOL folder must be located on an NTFS volume.  |
| Enter a location for the SYSVOL folder.   |
| Eolder location:  |
| C:NWINDOWS\SYSVOL Bjowse  |
|   |
|   |
|   |
|   |
|   |
| < <u>B</u> ack <u>N</u> ext> Cancel   |

11. 권한 페이지에서 Windows 2000 또는 Windows Server 2003 운영 체제와만 호환되는 권한이 선택되었는지 확인하고 다음 을 클릭합니다

| Active Directory Installation Wizard   |
|--|
| Permissions<br>Select default permissions for user and group objects.  |
| Some server programs, such as Windows NT Remote Access Service, read information<br>stored on domain controllers.  |
| Permissions compatible with pre-Windows 2000 server operating systems<br>Select this option if you run server programs on pre-Windows 2000 server operating<br>systems or on Windows 2000 or Windows Server 2003 operating systems that are<br>members of pre-Windows 2000 domains. Anonymous users can read information on this domain. |
| Permissions compatible only with Windows 2000 or Windows Server 2003<br>operating systems Select this option if you run server programs only on Windows 2000 or Windows<br>Server 2003 operating systems that are members of Active Directory domains. Only<br>authenticated users can read information on this domain.                  |
| < <u>B</u> ack <u>N</u> ext> Cancel  |

12. 디렉터리 서비스 복원 모드 관리 암호 페이지에서 암호 상자를 비워 두고 다음을 **클릭합니다**. 13. Summary(요약) 페이지의 정보를 검토하고 Next(**다음**)를 클릭합니다

| Summaru                  |   | ~    |
|--------------------------|---|------|
| Revie                    | w and confirm the options you selected.   |      |
| You d                    | nose to:  |      |
| The n                    | ew domain name is example.com. This is also the name of the new forest.   |      |
| The N                    | etBIOS name of the domain is EXAMPLE  |      |
| Datab<br>Log fil<br>SYSV | ase folder: C:\WINDOWS\NTDS<br>e folder: C:\WINDOWS\NTDS<br>DL folder: C:\WINDOWS\SYSVDL  |      |
| The D<br>will be         | NS service will be installed and configured on this computer. This computer<br>configured to use this DNS server as its preferred DNS server. |      |
| The p<br>the ac          | assword of the new domain administrator will be the same as the password of<br>ministrator of this computer.                                  |      |
| To ch                    | ange an option, click Back. To begin the operation, click Next.   |      |
|                          |   |      |
|                          | < <u>Back</u> <u>N</u> ext> Cance   | el l |

- 14. Active Directory 설치가 완료되면 Finish(마침)를 클릭합니다.
- 15. 컴퓨터를 다시 시작하라는 메시지가 표시되면 지금 다시 시작을 클릭합니다.

#### <u>도메인 기능 수준 올리기</u>

- 1. 관리 도구 폴더(시작 > 프로그램 > 관리 도구 > Active Directory 도메인 및 트러스트)에서 Active Directory 도메인 및 트러스트 스냅인을 열고 도메인 컴퓨터 CA.demo.local을 마우스 오른쪽 단추로 클릭합니다.
- 2. 도메인 **기능 수준 올리기**를 클릭한 다음 도메인 기능 수준 올리기 페이지에서 Windows Server 2003을 선택합니다

| Raise Domain Functional Level   | x |
|---|---|
| Domain name:  |   |
| demo.local  |   |
| Current domain functional level:  |   |
| Windows 2000 mixed  |   |
| Select an available domain functional level:  |   |
|   | 1 |
| Windows Server 2003   | 1 |
| After you raise the domain functional level, it cannot be reversed. For more information on domain functional levels, click Help. |   |
|   |   |
|   |   |
| <u>R</u> aise Cancel <u>H</u> elp   |   |

3. Raise(올리기)를 클릭하고 OK(확인)를 클릭한 다음 OK(확인)를 다시 클릭합니다.

#### <u>DHCP 설치 및 구성</u>

- 1. 제어판**의 프로그램 추가/제거**를 사용하여 DHCP(Dynamic Host Configuration Protocol)를 네 트워킹 서비스 구성 요소로 설치합니다.
- 2. Administrative Tools 폴더(시작 > Programs > Administrative Tools > DHCP)에서 DHCP 스냅 인을 열고 DHCP 서버, CA.demo.local을 강조 표시합니다.
- 3. DHCP **서비스**에 권한을 부여하려면 Action(작업)과 **Authorize(**권한 부여)를 차례로 클릭합니 다.
- 콘솔 트리에서 CA.demo.local을 마우스 오른쪽 단추로 클릭한 다음 New Scope(새 범위)를 클 릭합니다.
- 5. 새 범위 마법사의 시작 페이지에서 다음을 클릭합니다.
- 6. Scope Name(범위 이름) 페이지의 Name(이름) 필드에 CorpNet을 입력합니다

| New Scope Wizard                              |   |
|---|---|
| Scope Name<br>You have to p<br>providing a de | provide an identifying scope name. You also have the option of scription.                                       |
| Type a name<br>how the scop                   | and description for this scope. This information helps you quickly identify<br>e is to be used on your network. |
| N <u>a</u> me:                                | CorpNet   |
| Description:                                  |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |
|   | < Back Next > Cancel  |
|   |   |

7. **다음**(Next)을 클릭하고 다음 매개변수를 입력합니다.시작 IP 주소 - 10.0.20.1끝 IP 주소 - 10.0.20.200길이 - 24서브넷 마스크 - 255.255.255.0

| New Scope Wizard  |  |  |  |  |  |
|---|--|--|--|--|--|
| IP Address Range<br>You define the scope address range by identifying a set of consecutive IP<br>addresses.   |  |  |  |  |  |
| Enter the range of addresses that the scope distributes.  |  |  |  |  |  |
| Start IP address: 10 . 0 . 20 . 1   |  |  |  |  |  |
| End IP address: 10 . 0 . 20 . 200   |  |  |  |  |  |
| A subnet mask defines how many bits of an IP address to use for the network/subnet<br>IDs and how many bits to use for the host ID. You can specify the subnet mask by<br>length or as an IP address. |  |  |  |  |  |
| Length: 24  |  |  |  |  |  |
| Sybnet mask: 255 . 255 . 0  |  |  |  |  |  |
|   |  |  |  |  |  |
|   |  |  |  |  |  |
| < <u>B</u> ack <u>N</u> ext > Cancel  |  |  |  |  |  |

8. Next(**다음)**를 클릭하고 Start IP(시작 IP) 주소로 *10.0.20.1*을 입력하고 End IP(끝 IP) 주소로 제 외할 *10.0.20.100*을 입력합니다. 그런 다음 Next(**다음**)를 클릭합니다. 이렇게 하면 10.0.20.1~10.0.20.100 범위의 IP 주소가 예약됩니다. 이러한 예약 IP 주소는 DHCP 서버에서 할당되지 않습니다

| Sco | ope Wizard  |
|-----|---|
| Add | Exclusions<br>Exclusions are addresses or a range of addresses that are not distributed by the<br>server.                                 |
|     | Type the IP address range that you want to exclude. If you want to exclude a single<br>address, type an address in Start IP address only. |
| 1   | Start IP address:         End IP address:           10.0.20.1         10.0.20.100   |
| I   | Excluded address range:   |
|     | Remove  |
|     |   |
|     |   |
|     |   |
|     | ( Rack Next ) Cancel  |
|     |   |

- 9. Lease Duration(리스 기간) 페이지에서 Next(**다음**)를 클릭합니다.
- 10. Configure DHCP Options(DHCP 옵션 구성) 페이지에서 Yes, I want to configure these options now(예, 지금 이 옵션을 구성하겠습니다)를 선택하고 Next(다음)를 클릭합니다

| New Scope Wizard   |                                       |  |  |  |
|--|---------------------------------------|--|--|--|
| <b>Configure DHCP Options</b><br>You have to configure the most common DHC<br>scope.   | CP options before clients can use the |  |  |  |
| When clients obtain an address, they are given DHCP options such as the IP<br>addresses of routers (default gateways), DNS servers, and WINS settings for that<br>scope. |                                       |  |  |  |
| The settings you select here are for this scope and override settings configured in the<br>Server Options folder for this server.  |                                       |  |  |  |
| Do you want to configure the DHCP options for this scope now?  |                                       |  |  |  |
| Yes, I want to configure these options not   |                                       |  |  |  |
| O No, I will configure these options later   |                                       |  |  |  |
|  |                                       |  |  |  |
|  |                                       |  |  |  |
|  |                                       |  |  |  |
|  |                                       |  |  |  |
|  | < <u>B</u> ack <u>N</u> ext > Cancel  |  |  |  |
|  |                                       |  |  |  |

11. Router (Default Gateway)(라우터(기본 게이트웨이)) 페이지에서 기본 라우터 주소 *10.0.20.1을* 추가하고 Next(**다음**)를 클릭합니다

.

| New Scope Wizard   |  |  |  |
|--|--|--|--|
| Router (Default Gateway)<br>You can specify the routers, or default gateways, to be distributed by this scope. |  |  |  |
| To add an IP address for a router used by clients, enter the address below.                                    |  |  |  |
| I <u>P</u> address:  |  |  |  |
| 10 . 0 . 20 . 1 Add  |  |  |  |
| <u>R</u> emove   |  |  |  |
|  |  |  |  |
| Down   |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| < <u>B</u> ack <u>N</u> ext > Cancel   |  |  |  |

12. Domain Name and DNS Servers(도메인 이름 및 DNS 서버) 페이지의 Parent domain(상위 도메인) 필드에 *demo.local을* 입력하고 IP address(IP 주소) 필드에 *10.0.10.10*을 입력한 다 음 Add(추가)를 **클릭하고 Next(다음)**를 클릭합니다

.

| New Scope Wizard   |                                     |      |  |  |
|--|-------------------------------------|------|--|--|
| Domain Name and DNS Servers<br>The Domain Name System (DNS) maps and translates domain names used by<br>clients on your network. |                                     |      |  |  |
| You can specify the parent domain you want the client computers on your network to use for DNS name resolution.                  |                                     |      |  |  |
| Parent do <u>m</u> ain: demo.local   |                                     |      |  |  |
| To configure scope clients to use DNS servers on your network, enter the IP addresses for those<br>servers.                      |                                     |      |  |  |
| <u>S</u> erver name:   | I <u>P</u> address:                 |      |  |  |
|  | A <u>d</u> d                        |      |  |  |
| R <u>e</u> solve   | 10.0.10.10 <u>R</u> emove           |      |  |  |
|  | Up                                  |      |  |  |
|  | Down                                |      |  |  |
|  |                                     |      |  |  |
|  | < <u>B</u> ack <u>N</u> ext > Cance | el 🔤 |  |  |

- 13. WINS Servers(WINS 서버) 페이지에서 Next(**다음**)를 클릭합니다.
- 14. Activate Scope(범위 활성화) 페이지에서 Yes, I want to activate this scope now(예, 지금 이 범위를 활성화하겠습니다)를 선택하고 Next(다음)를 클릭합니다

| New Scope Wizard  |                   |                |        |
|---|-------------------|----------------|--------|
| Activate Scope<br>Clients can obtain address leases only if a so  | cope is activated |                | (C)    |
| Do you want to activate this scope now?<br>Yes, I want to activate this scope now<br>No, I will activate this scope later |                   |                |        |
|   | < <u>B</u> ack    | <u>N</u> ext > | Cancel |

15. New Scope Wizard(새 범위 마법사) 페이지를 마치면 Finish(마침)를 클릭합니다.

#### <u>인증서 서비스 설치</u>

다음 단계를 수행합니다.

**참고:** 인증서 서비스를 설치하기 전에 IIS를 설치해야 하며 사용자가 엔터프라이즈 관리자 OU의 일 부여야 합니다.

- 1. 제어판에서 [프로그램 추가/제거]를 연 다음 [Windows 구성 요소 추가/제거]를 클릭합니다.
- 2. Windows 구성 요소 마법사 페이지에서 인증서 서비스를 선택하고 다음을 클릭합니다.
- 3. CA Type(CA 유형) 페이지에서 Enterprise root CA(엔터프라이즈 루트 CA)를 선택하고 Next(다음)를 클릭합니다.
- 4. CA Identifying Information(CA 식별 정보) 페이지의 *Common* name for this CA(이 CA의 공통 이름) 상자에 democa를 입력합니다. 기타 선택 사항인 세부사항도 입력할 수 있습니다. 그런 다음 **다음**을 클릭하고 Certificate Database Settings 페이지에서 기본값을 수락합니다.
- 5. Next(다음)를 클릭합니다. 설치가 완료되면 Finish(마침)를 클릭합니다.
- 6. IIS 설치에 대한 경고 메시지를 읽은 후 확인을 클릭합니다.

#### <u>인증서에 대한 관리자 권한 확인</u>

- 1. 시작 > 관리 도구 > 인증 기관을 선택합니다.
- 2. democa CA를 마우스 오른쪽 버튼으로 클릭한 다음 Properties(속성)를 클릭합니다.

- 3. Security(보안) 탭의 Group or User names(그룹 또는 사용자 이름) 목록에서 Administrators(관리자)를 클릭합니다.
- 4. Permissions for Administrators(관리자 권한) 목록에서 다음 옵션이 Allow(허용)로 설정되어 있는지 확인합니다.인증서 발급 및 관리CA 관리인증서 요청이 중 하나라도 Deny(거부)로 설정되거나 선택되지 않은 경우, Permissions(권한)를 Allow(허용)로 설정합니다

| ca.demo.local Properties  |                                     | ? ×                          |
|---|-------------------------------------|------------------------------|
| General Policy Module Exit Mod<br>Certificate Managers Restrictions Auditin   | lule   Extension<br>ng   RecoveryAg | ns Storage<br>gents Security |
| <u>G</u> roup or user names:<br>Administrators (DEMO\Administrators<br>Authenticated Users<br>Domain Admins (DEMO\Domain Admins<br>Enterprise Admins (DEMO\Enterprise | )<br>nins)<br>: Admins)             |                              |
| Permissions for Administrators  | A <u>d</u> d<br>Allow               | <u>R</u> emove<br>Deny       |
| Read<br>Issue and Manage Certificates<br>Manage CA<br>Request Certificates  |                                     |                              |
| OK  | Cancel                              | Apply                        |

5. OK(**확인**)를 클릭하여 democa CA Properties(데모 CA 속성) 대화 상자를 닫은 다음 Certification Authority(인증 기관)를 닫습니다.

#### <u>도메인에 컴퓨터 추가</u>

다음 단계를 수행합니다.

**참고:** 컴퓨터가 이미 도메인에 추가된 경우 도메인에 사용자 <u>추가를 진행합니다</u>.

- 1. Active Directory 사용자 및 컴퓨터 스냅인을 엽니다.
- 2. 콘솔 트리에서 demo.local을 확장합니다.
- 3. 컴퓨터를 마우스 오른쪽 단추로 **클릭하고 새로 만들기**를 클릭한 다음 컴퓨터를 **클릭합니다**.

4. 새 개체 - 컴퓨터 대화 상자의 컴퓨터 이름 필드에 컴퓨터 이름을 입력하고 다음을 **클릭합니다**. 이 예에서는 컴퓨터 이름 Client를 *사용합니다* 

| lew Object - Computer   | × |
|---|---|
| Create in: demo.local/Users                                     |   |
| Computer name:  |   |
| client  |   |
| Computer name (pre-Windows 2000):                               |   |
| CLIENT  |   |
| The following user or group can join this computer to a domain. |   |
| User or group:  |   |
| Default: Domain Admins Change                                   |   |
| Assign this computer account as a pre-Windows 2000 computer     |   |
| Assign this computer account as a backup domain controller      |   |
|   |   |
| < Back Next > Cancel  | _ |
|   |   |

- 5. Managed(관리됨) 대화 상자에서 Next(다음)를 클릭합니다.
- 6. 새 개체 컴퓨터 대화 상자에서 마침을 클릭합니다.
- 7. 추가 컴퓨터 계정을 생성하려면 3단계부터 6단계까지 반복합니다.

#### 컴퓨터에 대한 무선 액세스 허용

- Active Directory 사용자 및 컴퓨터 콘솔 트리에서 컴퓨터 폴더를 클릭하고 무선 액세스를 할당 할 컴퓨터를 마우스 오른쪽 단추로 클릭합니다. 이 예에서는 7단계에서 추가한 computer Client의 절차를 보여줍니다. 속성을 클릭한 다음 전화 접속 탭으로 이동합니다.
- 2. Remote Access Permission(원격 액세스 권한)에서 Allow access(**액세스 허용)**를 선택하고 **OK(확인)**를 클릭합니다

| client Properties ? 🗙  |
|--|
| General Operating System Member Of Location Managed By Dial-in |
| Remote Access Permission (Dial-in or VPN)                      |
|  |
| © <u>D</u> eny access  |
| C Control access through Remote Access Policy                  |
|  |
| Callback Options   |
| No <u>C</u> allback  |
| Set by Caller (Routing and Remote Access Service only)         |
| C Always Callback to:  |
| Assign a Static IP Address                                     |
| Apply Static <u>R</u> outes                                    |
| Define routes to enable for this Dial-in <u>Static Routes</u>  |
|  |
| OK Cancel <u>Apply</u>   |

<u>도메인에 사용자 추가</u>

- 1. Active Directory 사용자 및 컴퓨터 콘솔 트리에서 사용자를 마우스 오른쪽 단추로 클릭하고 **새 로 만들기**를 클릭한 다음 **사용자**를 **클릭합니다**.
- 2. New Object User(새 개체 사용자) 대화 상자에서 무선 사용자의 이름을 입력합니다. 이 예 에서는 이름 필드에 *wirelessuser*라는 이름을 사용하고 사용자 로그온 이름 *필드*에 wirelessuser라는 이름을 사용합니다. **Next(다음)**를 클릭합니다

| New Object - User 🛛 🔀                              |
|--|
| Create in: demo.local/Users                        |
| <u>F</u> irst name: wirelessuser <u>I</u> nitials: |
| Last name:   |
| Full n <u>a</u> me: wirelessuser                   |
| <u>U</u> ser logon name:<br>wirelessuser           |
| User logon name (pre- <u>W</u> indows 2000):       |
| DEMO\ wirelessuser                                 |
|  |
| < <u>B</u> ack <u>N</u> ext > Cancel               |

3. New Object - User(새 개체 - 사용자) 대화 상자의 Password(비밀번호) 및 Confirm password(비밀번호 확인) 필드에 원하는 비밀번호를 입력합니다. 사용자가 **다음 로그온 시 암** 호를 변경해야 함 확인란의 선택을 취소하고 **다음** 을 클릭합니다

| Create in: demo.local/Users           Password:         ••••••••   |  |
|--|--|
| Password:  |  |
| Confirm password:  |  |
| <ul> <li>User <u>m</u>ust change password at next logon</li> <li>U<u>s</u>er cannot change password</li> <li>Pass<u>w</u>ord never expires</li> <li>Account is disabled</li> </ul> |  |
|  |  |

4. 새 개체 - 사용자 대화 상자에서 마침을 클릭합니다.

5. 추가 사용자 계정을 생성하려면 2~4단계를 반복합니다.

#### <u>사용자에 대한 무선 액세스 허용</u>

- 1. Active Directory 사용자 및 컴퓨터 콘솔 트리에서 **사용자** 폴더를 클릭하고 **무선 사용자**를 마우 스 오른쪽 단추로 클릭한 다음 **속성**을 클릭한 다음 **전화 접속 탭으로** 이동합니다.
- 2. Remote Access Permission(원격 액세스 권한)에서 Allow access(**액세스 허용)**를 선택하고 **OK(확인)**를 클릭합니다

| irelessuse   | Properti  | es                                   |                               |   | ?                                |
|--|---|--------------------------------------|-------------------------------|---|----------------------------------|
| Remote<br>General  <br>Member                              | e control<br>Address<br>Of  | Account Dial-in                      | inal Servic<br>Profile<br>Env | ces Profile  <br>  Telephones  <br>ironment | COM+<br>Organization<br>Sessions |
| Remote /<br>C Allow<br>C Deny<br>C Contr                   | Access Per<br>access<br>access<br>of access th                    | mission (Dial-i<br>hrough Remo       | n or VPN)                     | Policy                                      |                                  |
| Callback<br>Callback<br>C No <u>C</u><br>C Set b<br>C Alwa | Caller-ID:<br>Options —<br>allback<br>y Caller (Ro<br>vs Callback | outing and Re                        | mote Acce                     | ess Service only)                           |                                  |
| C Assig<br>Apply<br>Define r<br>connec                     | n a Static II<br>Static <u>R</u> ou<br>outes to en<br>tion.       | P Address<br>tes<br>hable for this E | i<br>Dial-in                  | Static Rou                                  | tes                              |
|  |   |                                      | ОК                            | Cancel                                      | Apply                            |

<u>도메인에 그룹 추가</u>

- 1. Active Directory 사용자 및 컴퓨터 콘솔 트리에서 사용자를 마우스 오른쪽 단추로 클릭하고 **새 로 만들기**를 클릭한 다음 그룹을 클릭합니다.
- 2. 새 개체 그룹 대화 상자의 그룹 이름 필드에 그룹 이름을 입력하고 확인을 **클릭합니다**. 이 문 서에서는 그룹 이름인 wirelessusers를 *사용합니다*

| ew Object - Group                         |                | × |
|---|----------------|---|
| Create in: dem                            | o.local/Users  |   |
| Group name:                               |                |   |
| wirelessusers                             |                |   |
| Consum a series (series 11) for days of 0 | 000).          |   |
| Group name (pre- <u>windows</u> 2         |                |   |
| 1   |                |   |
| Group scope                               | Group type     |   |
| C Domain local                            | Security       |   |
| Global                                    | C Distribution |   |
| C Universal                               |                |   |
|   |                |   |
|   |                |   |
|   | OK Cance       | 1 |
|   |                |   |

#### <u>무선 사용자 그룹에 사용자 추가</u>

다음 단계를 수행합니다.

- 1. Active Directory 사용자 및 컴퓨터의 세부 정보 창에서 WirelessUsers 그룹을 두 번 *클릭합니 다*.
- 2. Members(구성원) 탭으로 이동하여 Add(추가)를 클릭합니다.
- 3. 사용자, 연락처, 컴퓨터 또는 그룹 선택 대화 상자에서 그룹에 추가할 사용자의 이름을 입력합 니다. 이 예에서는 그룹에 사용자 무선사용자를추가하*는 방법*을 보여줍니다. **OK(확인)**를 클릭

| Select this object type.  | Object Trees      |
|---|-------------------|
| Users or Uther objects  | Ubject Types      |
| From this location:   |                   |
| idemo.local   | Locations         |
|   |                   |
| Enter the object names to select ( <u>examples</u> ):                 |                   |
| Enter the object names to select ( <u>examples)</u> :<br>wirelessuser |                   |
| Enter the object names to select ( <u>examples</u> ):<br>wirelessuser |                   |
| Enter the object names to select ( <u>examples</u> ):<br>wirelessuser | <u>Check Name</u> |

합니다.

4. Multiple Names Found 대화 상자에서 OK를 **클릭합니다**. 무선 사용자 사용자 계정이 무선 사용자 그룹에 추가됩니다

| wirelessusers Properties             | ? × |
|--------------------------------------|-----|
| General Members Member Of Managed By |     |
| Members:                             |     |
| Name Active Directory Folder         |     |
| 🖸 🖸 Administrator demo.local/Users   |     |
| 🖸 😡 wirelessuser demo.local/Users    |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      |     |
|                                      | _   |
| Add Bemove                           |     |
|                                      |     |
|                                      |     |
| OK Cancel App                        | ply |

5. 무선사용자 **그룹**에 대한 변경 사항을 저장하려면 OK를 클릭합니다. 6. 그룹에 사용자를 더 추가하려면 이 절차를 반복합니다.

#### <u>무선 사용자 그룹에 클라이언트 컴퓨터 추가</u>

- 1. 이 문서의 WirelessUsers 그룹에 <u>사용자 추가 섹션</u>에서 1단계와 2단계를 반복합니다.
- 2. 사용자, 연락처 또는 컴퓨터 선택 대화 상자에서 그룹에 추가할 컴퓨터의 이름을 입력합니다. 이 예에서는 client라는 컴퓨터를 그룹에 추가하는 *방법*을 보여줍니다

| Users or Other objects             |                               | Object Types            |
|------------------------------------|-------------------------------|-------------------------|
| From this location:                |                               |                         |
| demo.local                         |                               | Locations               |
|                                    |                               |                         |
| Enter the object names t           | o select ( <u>examples</u> ): |                         |
| Enter the object names t<br>client | o select ( <u>examples)</u> : | <br><u>C</u> heck Names |

. 3. 개체 **유형**을 클릭하고 **사용자** 확인란의 선택을 취소한 다음 컴퓨터**를 선택합니다** 

| Object Types                                  | ? ×       |
|---|-----------|
| Select the types of objects you want to find. |           |
| Object types:                                 |           |
| V Other objects                               |           |
| Computers                                     |           |
|   |           |
|   |           |
|   |           |
|   |           |
| 1   |           |
|   | OK Cancel |
|   |           |

4. OK(**확인)를** 두 번 클릭합니다. CLIENT 컴퓨터 계정이 wirelessusers 그룹에 추가됩니다

| wirelessusers Proper | ties                    | ? ×   |
|----------------------|-------------------------|-------|
| General Members      | Member Of Managed By    |       |
| Members:             |                         |       |
| Name                 | Active Directory Folder |       |
| Administrator        | demo.local/Users        |       |
| - client             | demo.local/Computers    |       |
| 2 wirelessuser       | demo.local/Users        |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
|                      |                         |       |
| bbA                  | Bemove                  |       |
|                      | Trucke                  |       |
|                      |                         |       |
|                      | OK Cancel               | Apply |

5. 이 절차를 반복하여 그룹에 컴퓨터를 더 추가합니다.

## Cisco 1121 Secure ACS 5.1

### <u>CSACS-1121 Series Appliance를 사용한 설치</u>

CSACS-1121 어플라이언스는 ACS 5.1 소프트웨어와 함께 사전 설치됩니다. 이 섹션에서는 설치 프로세스 및 ACS를 설치하기 전에 수행해야 하는 작업에 대한 개요를 제공합니다.

- 1. CSACS-1121을 네트워크 및 어플라이언스 콘솔에 연결합니다. <u>4장 "케이블 연결"을</u> 참조하십 시오<u>.</u>
- 2. CSACS-1121 어플라이언스의 전원을 켭니다. <u>4장, "CSACS-1121 Series 어플라이언스 전원</u> <u>켜기"를</u> 참조하십시오<u>.</u>
- 3. CLI 프롬프트에서 setup 명령을 실행하여 ACS 서버의 초기 설정을 구성합니다. 설치 프로그 램 실행을 참조하십시오.

### <u>ACS 서버 설치</u>

이 섹션에서는 CSACS-1121 Series Appliance의 ACS 서버 설치 프로세스에 대해 설명합니다.

- <u>설치 프로그램 실행</u>
- <u>설치 프로세스 확인</u>
- <u>설치 후 작업</u>

Cisco Secure ACS Server 설치에 대한 자세한 내용은 <u>Cisco Secure Access Control System 5.18</u> 설치 및 업그레이드 가이드를 참조하십시오.

## Cisco WLC5508 컨트롤러 컨피그레이션

WPAv2/WPA에 필요한 구성을 만듭니다.

다음 단계를 수행합니다.

**참고:** 컨트롤러에는 네트워크에 대한 기본 연결이 있고 관리 인터페이스에 대한 IP 연결이 성공적이 라고 가정합니다.

1. 컨트롤러에 로그인하려면 https://10.0.1.10으로 **이동합니다** 



- 2. Login(로그인)을 클릭합니다.
- 3. 기본 사용자 admin 및 기본 비밀번호 admin으로 로그인합니다.
- 4. Controller(컨트롤러) 메뉴에서 VLAN 매핑을 위한 새 인터페이스를 생성합니다.
- 5. Interfaces를 클릭합니다.
- 6. **새로 만들기**를 클릭합니다.
- 7. Interface name 필드에 Employee를 *입력합니다*. (이 필드는 원하는 모든 값이 될 수 있습니다 .)
- 8. VLAN ID 필드에 20을 입력합니다. 이 필드는 네트워크에서 전송되는 모든 VLAN이 될 수 있습니다.
- 9. Apply를 클릭합니다.
- 10. 이 Interfaces(인터페이스) > Edit(편집) 창에 다음과 같은 정보가 표시됨에 따라 정보를 구성 합니다.인터페이스 IP 주소 - 10.0.20.2넷마스크 - 255.255.255.0게이트웨이 - 10.0.10.1기본 DHCP -

10.0.10.10

| սիսիս  |   |                                  | S                                  | a <u>v</u> e Configuration           | Ping   Log | pout   <u>R</u> efre |
|--|---|----------------------------------|------------------------------------|--------------------------------------|------------|----------------------|
|  | VLANS CONTROLLER  | WIRELESS                         | SECURITY                           | MANAGEMENT                           | COMMAND    | S HELP               |
| Controller   | Interfaces > Edit   |                                  |                                    | < 8                                  | ack        | Apply                |
| General<br>Inventory<br>Interfaces<br>Multicast                                  | General Informat  | tion<br>em                       | ployee                             |                                      | -          |                      |
| Network Routes <ul> <li>Internal DHCP Serv</li> <li>Mobility Manageme</li> </ul> | MAC Address<br>er<br>t  | 00:                              | 24:97:69:4d:e                      | 0                                    |            |                      |
| Ports<br>NTP<br>EDP  | Guest Lan<br>Quarantine<br>Quarantine Vian Id                 | 0                                |                                    |                                      |            |                      |
| Advanced   | Physical Informa<br>Port Number                               | tion                             | 2                                  |                                      |            |                      |
|  | Backup Port<br>Active Port<br>Enable Dynamic A                | P Management                     | 0                                  |                                      |            |                      |
|  | Interface Addres  | s                                |                                    |                                      |            |                      |
|  | VLAN Identifier<br>IP Address<br>Netmask                      |                                  | 20<br>10.0.20.2<br>255.255.255     | 0                                    |            |                      |
|  | Gateway<br>DHCP Informatio                                    | n                                | 10.0.20.1                          |                                      |            |                      |
|  | Secondary DHCP Se   | Server                           | 10.0.10.10                         |                                      |            |                      |
|  | Access Control L  | ist                              |                                    |                                      |            |                      |
|  | ACL Name  |                                  | none 💌                             |                                      | _          |                      |
|  | Note: Changing the I<br>temporarily disabled<br>some clients. | nterface param<br>and thus may r | eters causes t<br>esult in loss of | he WLANs to be<br>f connectivity for |            |                      |

- 11. Apply를 클릭합니다.
- 12. WLANs(WLAN) **탭을** 클릭합니다.
- 13. Create **New(새로 만들기)**를 선택하고 **Go(이동)**를 클릭합니다.
- 14. Profile Name(프로필 이름)을 입력하고 WLAN SSID 필드에 Employee(직원)를 *입력합니다*

| սիսիս          |       |              |          |          | Sa | ve Configuration | l <u>P</u> ing | Logou | ut   <u>R</u> efre |
|----------------|-------|--------------|----------|----------|----|------------------|----------------|-------|--------------------|
|                | WLANS |              | WIRELESS | SECURI   | TY | MANAGEMENT       | COMN           | ANDS  | HELP               |
| WLANs          | V     | VLANs > New  |          |          |    | < Ba             | ack            | A     | pply               |
| WLANS<br>WLANS |       | Туре         | [        | WLAN     | •  |                  |                |       |                    |
| Advanced       |       | Profile Name | t        | Employee |    |                  |                |       |                    |
|                |       | SSID         | 1        | Employee |    |                  |                |       |                    |
|                |       | ID           | [        | 1        |    |                  |                |       |                    |

15. WLAN의 ID를 선택하고 Apply를 **클릭합니다**.

- 16. WLANs(WLAN) > Edit(수정) 창이 나타나면 이 WLAN에 대한 정보를 구성합니다.참고: WPAv2는 이 실습에서 선택한 레이어 2 암호화 방법입니다. TKIP-MIC 클라이언트가 있는 WPA를 이 SSID에 연결하도록 허용하려면 WPA 호환성 모드 및 Allow WPA2 TKIP Clients(WPA2 TKIP 클라이언트 허용) 상자 또는 802.11i AES 암호화 방법을 지원하지 않는 클라이언트를 선택할 수도 있습니다.
- 17. WLANs(WLAN) > Edit(수정) 화면에서 General(일반) 탭을 클릭합니다.
- 18. Status(상태) 상자에 Enabled(활성화됨)가 **선택되어** 있고 적절한 Interface(employee)(인터 페이스(직원)가 선택되었는지 확인합니다. 또한 Broadcast SSID에 대해 Enabled(활성화됨) 확인란을 선택해야 합니다

| վուլո         |                                 |                                   |                                     | Sa                        | ave Configuration   | Ping           | Logout <u>R</u> efre |
|---------------|---------------------------------|-----------------------------------|-------------------------------------|---------------------------|---------------------|----------------|----------------------|
| CISCO MONITOR | WLANS CON                       | ROLLER W                          | IRELESS                             | SECURITY                  | MANAGEMENT          | C <u>O</u> MM/ | ANDS HELP            |
| WLANs         | WLANs                           | > Edit                            |                                     |                           | < B:                | ack            | Apply                |
| VLANs         | Genera                          | I Securit                         | y QoS                               | Advanc                    | ed                  |                |                      |
| Advanced      | Profil<br>Name                  | e Empl                            | oyee                                |                           |                     |                |                      |
|               | Туре                            | WLAP                              | N                                   |                           |                     |                |                      |
|               | SSID                            | Empl                              | oyee                                |                           |                     |                |                      |
|               | Statu                           | s 🗖 i                             | Enabled                             |                           |                     |                |                      |
|               | Secu<br>Polici                  | ity [WP/<br>as (Modif<br>chang    | A2][Auth(8<br>fications don<br>es.) | (02.1X)]<br>e under secur | ity tab will appear | r after app    | plying the           |
|               | Radio<br>Inter<br>Broad<br>SSID | Policy All<br>ace emp<br>cast F E | loyee 💌                             | e                         |                     |                |                      |

- 19. **보안** 탭을 클릭합니다.
- 20. Layer 2 하위 메뉴에서 Layer 2 Security에 대해 **WPA + WPA2**를 선택합니다. WPA2 암호화 의 경우 TKIP **클라이언트를** 허용하려면 AES **+ TKIP**를 선택합니다.
- 21. 인증 방법으로 **802.1**x를 선택합니다

| Security                        | QoS<br>AAA Se<br>WPA+WPA2               | Advance<br>ervers | ed<br>•                             |
|---------------------------------|---|-------------------|-------------------------------------|
| Layer 3<br>ecurity <sup>©</sup> | AAA Se                                  | ervers            | •                                   |
| ecurity 🙎 🛛                     | VPA+WPA2                                |                   | •                                   |
| Parameter                       | MAC Filte                               | ering             |                                     |
| y                               |   |                   |                                     |
| cy                              | 1                                       |                   |                                     |
| ryption                         | AE AE                                   | s 🔽               | ткія                                |
| Mgmt                            | 802.1                                   | LX .              | -                                   |
|                                 | Parameter<br>/<br>cy<br>ryption<br>Mgmt | Parameters        | Parameters V Cy Fyption Mgmt 802.1X |

- 22. 레이어 3 하위 메뉴는 필요 없으므로 건너뜁니다. RADIUS 서버가 구성되면 Authentication 메뉴에서 적절한 서버를 선택할 수 있습니다.
- 23. 특별한 구성**이** 필요하지 않는 한 QoS 및 Advanced 탭은 기본값으로 둘 수 있습니다.
- 24. RADIUS 서버를 추가 하려면 보안 메뉴를 클릭 합니다.
- 25. RADIUS 하위 메뉴에서 Authentication(인증)을 **클릭합니다**. 그런 다음 New(새로 만들기)를 클릭합니다.
- 26. 이전에 구성된 ACS 서버인 RADIUS 서버 IP 주소(10.0.10.20)를 추가합니다.
- 27. 공유 키가 ACS 서버에 구성된 AAA 클라이언트와 일치하는지 확인합니다. Network User(네 트워크 사용자) 상자가 선택되어 있는지 확인하고 Apply(적용)를 클릭합니다

| սիսիս   |  | Save Configuration   Ping   Logout Befree  |
|---|--|--|
| CISCO MONITOR WL  | ANS <u>C</u> ONTROLLER   | WIRELESS SECURITY MANAGEMENT COMMANDS HELP |
| Security  | RADIUS Authe   | ntication Servers > New < Back Apply       |
| <ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul> | Server Index<br>(Priority)<br>Server IP<br>Address<br>Shared Secret<br>Format<br>Shared Secret<br>Confirm<br>Shared Secret<br>Key Wrap |  |
| Local EAP   | Server Status  | Enabled 💌                                  |
| Priority Order  | Support for  | Enabled 💌                                  |
| Certificate   | Server Timeout   | 2 seconds                                  |
| Access Control Lists  | Network User   | Enable                                     |
| <ul> <li>Wireless Protection</li> <li>Policies</li> </ul>   | Management   | Enable                                     |
| Web Auth  | IPSec  | Enable Enable                              |
| Advanced  |  |  |

28. 이제 기본 컨피그레이션이 완료되었으므로 PEAP 테스트를 시작할 수 있습니다.

## <u>PEAP 인증</u>

MS-CHAP 버전 2를 사용하는 PEAP에는 ACS 서버에는 인증서가 필요하지만 무선 클라이언트에 는 인증서가 필요하지 않습니다. ACS 서버의 컴퓨터 인증서 자동 등록을 사용하여 구축을 간소화 할 수 있습니다.

컴퓨터 및 사용자 인증서에 대한 자동 등록을 제공하도록 CA 서버를 구성하려면 이 섹션의 절차를 완료합니다.

**참고:** Microsoft는 Windows 2003 Enterprise CA 릴리스와 함께 웹 서버 템플릿을 변경하여 더 이상 키를 내보낼 수 없으며 옵션이 회색으로 비활성화되도록 했습니다. 서버 인증용 인증서 서비스와 함께 제공되는 다른 인증서 템플릿은 없으며 드롭다운에서 사용 가능한 키를 내보낼 수 있는 것으 로 표시할 수 있으므로 이를 수행하는 새 템플릿을 생성해야 합니다.

**참고:** Windows 2000에서는 내보낼 수 있는 키를 사용할 수 있으며 Windows 2000을 사용하는 경우 이러한 절차를 수행할 필요가 없습니다.

#### <u>인증서 템플릿 스냅인 설치</u>

- 1. 시작 > 실행을 선택하고 mmc를 *입력한* 다음 확인 을 클릭합니다.
- 2. 파일 메뉴에서 스냅인 추가/제거를 클릭한 다음 추가를 클릭합니다.
- 3. 스냅인에서 **인증서 템플릿** 을 두 번 클릭하고 **닫기** 를 클릭한 다음 **확인** 을 클릭합니다.
- 4. 콘솔 트리에서 Certificate Templates(인증서 템플릿)를 클릭합니다. 모든 인증서 템플릿이 Details(세부 정보) 창에 나타납니다.
- 5. 2~4단계를 우회하려면 certtmpl.msc를 입력하여 인증서 템플릿 스냅인을 엽니다

| 🌇 MyConsole - [Console Root\Ce           | rtificate Templates]                 |                           |
|--|--------------------------------------|---------------------------|
| 🚡 Elle Action View Favorites             | <u>W</u> indow <u>H</u> elp          | _8×                       |
|  |                                      |                           |
| Console Root                             | Template Display Name                | Minimum Supported CAs     |
| Certificate Templates                    | Exchange Signature Only              | Windows 2000              |
| -  | Exchange User                        | Windows 2000              |
|  | 1PSec                                | Windows 2000              |
|  | IPSec (Offline request)              | Windows 2000              |
|  | Key Recovery Agent                   | Windows Server 2003, En   |
|  | RAS and IAS Server                   | Windows Server 2003, En   |
|  | Root Certification Authority         | Windows 2000              |
|  | Router (Offline request)             | Windows 2000              |
|  | Smartcard Logon                      | Windows 2000              |
|  | Smartcard User                       | Windows 2000              |
|  | Subordinate Certification Authority  | Windows 2000              |
|  | Trust List Signing                   | Windows 2000              |
|  | 22 User                              | Windows 2000              |
|  | User Signature Only                  | Windows 2000              |
|  | Web Server                           | Windows 2000              |
|  | Workstation Authe Dyplicate Template | Windows Server 2003, En 🖵 |
|  | ▲ All Tasks ▶                        |                           |
| Using this template as a base, creates a | template that supports Properties    |                           |

## ACS 웹 서버용 인증서 템플릿 만들기

다음 단계를 수행합니다.

1. 인증서 템플릿 스냅인의 세부 정보 창에서 웹 서버 템플릿을 클릭합니다.

2. 작업 메뉴에서 템플릿 복제**를 클릭합니다** 

| Properties of New Template   | × |
|--|---|
| Issuance Requirements   Superseded Templates   Extensions   Securi<br>General   Request Handling   Subject Name                    | 2 |
| Template display name:<br>Copy of Web Server   |   |
| Minimum Supported CAs: Windows Server 2003, Enterprise Edition   |   |
| After you apply changes to this tab, you can no longer change the template<br>name.  | , |
| Iemplate name:<br>Copy of Web Server   | - |
|  |   |
| Validity period:     Renewal period:       2     years     6   |   |
| Publish certificate in Active Directory     Do not automatically reenrol if a duplicate certificate exists in Active     Directory |   |
|  |   |
| OK Cancel Apply  |   |

3. Template display name(템플릿 표시 이름) 필드에 ACS를 *입력합니다* 

| operties of                | New Templa                                  | ite   |                                   | ?                         |
|----------------------------|---|---|-----------------------------------|---------------------------|
| Issuance Re<br>Genera      | quirements                                  | Superseded Templa<br>Request Handling       | ites   Extensio<br>  Subj         | ons   Securit<br>ect Name |
| Template d                 | splay name:                                 |   |                                   |                           |
| Minimum Su<br>After you ap | upported CAs:<br>oply changes to            | Windows Server 20<br>o this tab, you can no | 03, Enterprise E<br>longer change | dition<br>the template    |
| name.                      |   |   |                                   |                           |
|                            | anie.                                       |   |                                   |                           |
| ⊻alidity peri<br>2 ye      | od:<br>ars 💌                                | Benewal p                                   | eriod:<br>eeks 💌                  |                           |
| Eublish                    | certificate in A<br>tot automatica<br>ctory | ctive Directory<br>ly reenroll if a duplica | te certificate ex                 | ists in Active            |
|                            |   | OK .  | Cancel                            | Apply                     |

4. Request Handling(요청 처리) 탭으로 이동하여 Allow private key to be exported(개인 키 내보

내기 허용)를 선택합니다. 또한 Purpose 드롭다운 메뉴에서 Signature and Encryption이 선택

| Issuance Regu                     | irements   Superseded Templates   Extensions   Securit                                  |
|-----------------------------------|---|
| General                           | Request Handling Subject Name   |
| Purpose:                          | Signature and encryption  |
|                                   | Archive subject's encryption private key  |
|                                   | Include symmetric algorithms allowed by the subject                                     |
|                                   | Delete revoked or expired certificates (do not archive)                                 |
| <u>M</u> inimum key s             | size: 1024 💌  |
|                                   | te key to be exported   |
| in Fight bird                     | ne rey to be exported   |
| Do the followir<br>associated wit | ng when the subject is enrolled and when the private key<br>h this certificate is used: |
| 🖲 <u>E</u> nroll subj             | ect without requiring any user input  |
| C Prompt the                      | suser during enrollment   |
| C Prompt the private key          | user during enrollment and require user input when the<br>v is used                     |
|                                   |   |

5. Requests must **use a following CSPs(요청에서 다음 CSP 중 하나를 사용해야 함)를** 선택하고 **Microsoft Base Cryptographic Provider v1.0을** 확인합니다. 선택된 다른 CSP의 선택을 취소 하고 OK(**확인**)를 클릭합니다

| P Selection   |
|---|
| Choose which cryptographic service providers (CSPs) can be used in<br>requests: |
| C <u>R</u> equests can use any CSP available on the subject's computer          |
| Requests must use one of the following CSPs:                                    |
| <u>C</u> SPs:   |
| Gemplus GemSAFE Card CSP v1.0   |
| Infineon SICRYPT Base Smart Card CSP  |
| ✓Microsoft Base Cryptographic Provider v1.0                                     |
| Microsoft Base DSS and Diffie-Hellman Cryptographic Provider                    |
| Microsoft DH SChannel Cryptographic Provider                                    |
| Microsoft Enhanced Cryptographic Provider v1.0                                  |
| Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Prov                    |
| Microsoft Enhanced RSA and AES Cryptographic Provider                           |
| Microsoft BSA SChannel Cryptographic Provider                                   |
|   |
| OK Cancel   |
|   |
|   |
| OK Cancel Apply   |

. 6. Subject **Name(주체 이름)** 탭으로 이동하여 요청에서 **Supply(공급**)를 선택하고 **OK(확인)**를 클

| General       Request Handling       Subject Name         © Supply in the request       Select this option to allow a variety of subject name formats or if y not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.         © Build from this Active Directory information         Select this option to enforce consistency among subject names and simplify certificate administration.         Subject name format:         None         Include e-mail name in subject name         Include this information in alternate subject name:         E-mail name         DNS name | Issuance Requirem  | ents   Superseded Templa  | tes Extensions Se   |
|---|--|---|---|
| <ul> <li>Supply in the request</li> <li>Select this option to allow a variety of subject name formats or if y not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.</li> <li>Build from this Active Directory information</li> <li>Select this option to enforce consistency among subject names and simplify certificate administration.</li> <li>Subject name format:         <ul> <li>None</li> <li>Include e-mail name in subject name</li> <li>Include this information in alternate subject name:</li> <li>E-mail name</li> <li>DNS name</li> </ul> </li> </ul>            | General  | Request Handling  | Subject Name  |
| Select this option to enforce consistency among subject names an simplify certificate administration. Subject name format: None Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name  | <ul> <li>Supply in the results of the second se</li></ul> | equest<br>ion to allow a variety of subje<br>ess to the domain of which the<br>t is not allowed if you choose<br>Active Directory information | ct name formats or if you<br>e subject is a member.<br>this option. |
| None       Image: Second state         Include e-mail name in subject name         Include this information in alternate subject name:         E-mail name         DNS name   | Select this optio<br>simplify certifical<br>Subject name for   | n to enforce consistency am<br>te administration.<br>ormat:   | ong subject names and t   |
| Include e-mail name in subject name Include this information in alternate subject name: E-mail name DNS name  | None   |   | Ŧ   |
| Include this information in alternate subject name:   |  | ail name in subject name  |   |
| E-mail name<br>DNS name   | Include em   | sai manne in estapeles manne  |   |
| DNS name  | Include this info  | rmation in alternate subject n  | ame:  |
| -   | Include this info  | rmation in alternate subject n  | ame:  |
| User prinicipal name (UPN)  | Include this info  | rmation in alternate subject n  | ame:  |
| Service principal name (SPN)  | Include this info  | rmation in alternate subject n<br>:<br>pal name (UPN)   | ame:  |
|   | Include this info  | rmation in alternate subject n<br>:<br>pal name (UPN)<br>cipal name (SPN)   | ame:  |
|   | Include this info  | rmation in alternate subject n<br>;<br>pal name (UPN)<br>cipal name (SPN)   | ame:  |

- 7. Security(보안) 탭으로 이동하여 Domain Admins Group(도메인 관리자 그룹)을 강조 표시하고 Allowed(허용)에서 Enroll(등록) 옵션이 선택되어 있는지 확인합니다.참고: 이 Active Directory 정보에서 빌드하도록 선택한 경우 UPN(User Principal Name)만 확인하고 Active Directory Users and Computers 스냅인의 무선 사용자 계정에 대한 전자 메일 이름이 입력되지 않았으 므로 Include email name in subject name and E-mail name(주체 이름과 전자 메일 이름에 전 자 메일 이름 포함)의 선택을 취소합니다. 이 두 옵션을 비활성화하지 않으면 자동 등록에서 전 자 메일을 사용하려고 시도하므로 자동 등록 오류가 발생합니다.
- 8. 필요한 경우 인증서가 자동으로 푸시되지 않도록 추가 보안 조치가 있습니다. 이러한 정보는 Issuance Requirements(발급 요건) 탭에서 확인할 수 있습니다. 이 문서에서는 이에 대해 자세

| Requ<br>F C | ice Requirements<br>ice the following for<br>A certificate manag | Superseded Templates<br>enrollment:<br>er approval | Extensions Securi       |
|-------------|--|--|-------------------------|
| Requ<br>C   | ire the following for<br>A certificate manag                     | enrollment:<br>er approval                         |                         |
|             | A certificate manag  | enroliment:<br>er approval                         |                         |
|             | A certificate manag  | er approval  |                         |
|             |  |  | _                       |
|             | his number of autho  | rized signatures:                                  |                         |
| 1           | f you require more th  | nan one signature, autoenro                        | ollment is not allowed. |
| F           | olicy type required in   | n signature:                                       |                         |
| Γ           |  |  | ¥                       |
| A           | pplication policy:   |  |                         |
| Γ           |  |  | Y                       |
| l           | suance policies:   |  | -                       |
|             |  |  | A <u>d</u> d            |
|             |  |  | Bemove                  |
|             |  |  |                         |

히 다루지 않습니다. └

9. 템플릿을 저장하고 Certificate Authority 스냅인에서 이 템플릿을 발급하는 단계로 이동하려면 OK(확인)를 클릭합니다.

### <u>새 ACS 웹 서버 인증서 템플릿 활성화</u>

- 1. 인증 기관 스냅인을 엽니다. Create the <u>Certificate Template for the ACS Web Server(ACS 웹 서버용 인증서 템플릿 생성) 섹션</u>에서 1~3단계를 수행하고 **Certificate Authority(인증 기관) 옵 션을** 선택하고 Local Computer(로컬 컴퓨터)를 선택한 다음 Finish(마침)를 클릭합니다.
- 2. Certificate Authority(인증 기관) 콘솔 트리에서 **ca.demo.local**을 확장한 다음 Certificate Templates(**인증서 템플릿**)를 마우스 오른쪽 버튼으로 **클릭합니다**.
- 3. New(새로 만들기) > Certificate Template to Issue(인증서 템플릿)로 이동합니다
| 📴 Certification Authority           |   |
|-------------------------------------|---|
| Eile Action View Help               |   |
|                                     |   |
| 🔯 Certification Authority (Local)   | Name  |
| 🖻 😰 ca.demo.local                   | Directory Email Replication                       |
|                                     | 2 Domain Controller Authentication                |
| Issued Certificates                 | EFS Recovery Agent                                |
| Pending Requests                    | Basic EFS   |
|                                     | 🛛 🔯 Domain Controller                             |
|                                     | Server  |
|                                     | huter   |
| <u>N</u> ew                         | <ul> <li>Certificate Template to Issue</li> </ul> |
| View                                | rdinate Certification Authority                   |
|                                     | histrator   |
| Refresh                             | 1   |
| Export                              | <u>L</u> ist                                      |
| Help                                |   |
| Refresh<br>Export  <br><u>H</u> elp | List  |

4. ACS Certificate Template(ACS 인증서 템플릿)을 클릭합니다

| Name  | Intended Purpose                      |  | - |
|---|---------------------------------------|--|---|
| R ACS                                       | Server Authentication                 |  |   |
| Authenticated Session                       | Client Authentication                 |  |   |
| 🙀 CA Exchange                               | Private Key Archival                  |  |   |
| CEP Encryption                              | Certificate Request Agent             |  |   |
| 🙀 Code Signing                              | Code Signing                          |  |   |
| Cross Certification Authority               | <alb< td=""><td></td><td></td></alb<> |  |   |
| 🗱 Enrollment Agent                          | Certificate Request Agent             |  |   |
| 🗱 Enrollment Agent (Computer)               | Certificate Request Agent             |  |   |
| Exchange Enrollment Agent (Offline request) | Certificate Request Agent             |  |   |
| 🗱 Exchange Signature Only                   | Secure Email                          |  | - |
| Sol Exchange Liser                          | Secure Email                          |  | • |

- 5. 확인을 클릭하고 Active Directory 사용자 및 컴퓨터 스냅인을 엽니다.
- 6. 콘솔 트리에서 Active Directory 사용자 및 컴퓨터를 두 번 클릭하고 demo.local을 마우스 오른 쪽 단추로 클릭한 다음 속성을 **클릭합니다**



7. Group Policy(그룹 정책) 탭에서 Default **Domain Policy(기본 도메인 정책)**를 클릭한 다음 Edit(수정)**를 클릭합니다**. 이렇게 하면 그룹 정책 개체 편집기 스냅인이 열립니다

| demo.local Properties  |                            | ? ×                 |
|--|----------------------------|---------------------|
| General Managed By Group Policy  |                            |                     |
| To improve Group Policy management, upgrade<br>Management Console (GPMC).<br>Current Group Policy Object Links for | to the Group Po<br>or demo | olicy               |
| Group Policy Object Links  | No Override                | Disabled            |
| Group Policy Objects higher in the list have the h<br>This list obtained from: AD2003.demo.local                   | ighest priority.           |                     |
| New         Add         Edit           Options         Delete         Properties                                   |                            | Up<br>Do <u>w</u> n |
| Block Policy inheritance   |                            |                     |
| Close  | Cancel                     | Apply               |

8. 콘솔 트리에서 Computer Configuration(컴퓨터 구성) > Windows Settings(Windows 설정) > Security Settings(보안 설정) > Public Key Policies(공개 키 정책)를 확장한 다음 Automatic Certificate Request Settings(자동 인증서 요청 설정)를 선택합니다

.



- 9. Automatic Certificate Request Settings(**자동 인증서 요청 설정)를 마우스 오른쪽 버튼**으로 클 릭하고 New(**새로 만들기**) > Automatic Certificate Request(**자동 인증서 요청)를** 선택합니다.
- 10. Welcome to the Automatic Certificate Request Setup Wizard(자동 인증서 요청 설정 마법사 시작) 페이지에서 Next(**다음**)를 클릭합니다.
- 11. Certificate Template(인증서 템플릿) 페이지에서 **Computer(컴퓨터)**를 클릭하고 **Next(다음** )를 클릭합니다

| tomatic Certificate Request Setup<br>Certificate Template<br>The next time a computer logs on, a<br>provided. | Wizard Exerciticate based on the template you select is   |
|---|---|
| A certificate template is a set of prec<br>computers. Select a template from th<br>Certificate templates:     | defined properties for certificates issued to<br>ne following list.   |
| Name  | Intended Purposes   |
| Computer<br>Domain Controller<br>Enrollment Agent (Computer)<br>IPSec   | Client Authentication, Server Authentication<br>Client Authentication, Server Authentication<br>Certificate Request Agent<br>IP security IKE intermediate |
| •   | <u> </u>  |
|   | < <u>B</u> ack <u>N</u> ext > Cancel  |

12. Automatic Certificate Request Setup Wizard(자동 인증서 요청 설정 마법사) 페이지를 완료 하면 Finish(마침)를 클릭합니다. 이제 그룹 정책 개체 편집기 스냅인의 세부 정보 창에 컴퓨 터 인증서 유형이 나타납니다

.

| 🚡 Group Policy Object Editor                          |                               |
|---|-------------------------------|
| Elle Action View Help                                 |                               |
|   |                               |
| S Default Domain Policy [AD2003.demo.local] Policy    | Automatic Certificate Request |
| E-B Computer Configuration                            | Computer                      |
| Software Settings                                     |                               |
| - Windows Settings                                    |                               |
| - Scripts (Startup/Shutdown)                          |                               |
| E-B Security Settings                                 |                               |
| Account Policies                                      |                               |
| Local Policies  |                               |
| Event Log   |                               |
| Restricted Groups                                     |                               |
| System Services                                       |                               |
| 🖲 🧰 Registry  |                               |
| 🕖 🛄 File System                                       |                               |
| Wireless Network (IEEE 802.11) Policies               |                               |
| 🖻 🚞 Public Key Policies                               |                               |
| Encrypting File System                                |                               |
|   |                               |
|   |                               |
| Enterprise Trust                                      |                               |
| Software Restriction Policies                         |                               |
| IP Security Policies on Active Directory (demo.local) |                               |
| Administrative Templates                              |                               |
| E- 🙀 User Configuration                               |                               |
| Software Settings                                     |                               |
| Windows Settings                                      |                               |
| Administrative Templates                              |                               |

- 13. 콘솔 트리에서 User Configuration(사용자 컨피그레이션) > Windows Settings(Windows 설정 ) > Security Settings(보안 설정) > Public Key Policies(공개 키 정책)를 확장합니다.
- 14. 세부 정보 창에서 Auto-enrollment Settings(자동 등록 설정)를 두 번 클릭합니다

| 🚡 Group Policy Object Editor                       |                         |
|--|-------------------------|
| <u>Eile Action View H</u> elp                      |                         |
|  |                         |
| 🗊 Default Domain Policy [AD2003.demo.local] Policy | Object Type             |
| 🗄 🜆 Computer Configuration                         | Enterprise Trust        |
| 🖻 🚛 User Configuration                             | Autoenrollment Settings |
| 🕀 💼 Software Settings                              |                         |
| 🖻 📲 Windows Settings                               |                         |
| - 🤧 Remote Installation Services                   |                         |
| Scripts (Logon/Logoff)                             |                         |
| 🖻 📲 📴 Security Settings                            |                         |
| 🚊 🔄 Public Key Policies                            |                         |
| Enterprise Trust                                   |                         |
| 🗄 💼 Software Restriction Policies                  |                         |
| 🕀 💼 Folder Redirection                             |                         |
| 主 🍘 Internet Explorer Maintenance                  |                         |
| 🗄 💼 Administrative Templates                       |                         |

15. Enroll certificates automatically(인증서 자동 등록)를 선택하고 Renew expired certificates(만 료된 인증서 갱신), Update pending certificates(보류 중인 인증서 업데이트), Remove revoked certificates(폐기된 인증서) 및 Update certificates that using certificates(인증서 템플 릿을 사용하는 인증서 업데이트)를 선택합니다

| Autoenrollment Settings Properties  | ? × |
|---|-----|
| General   |     |
| Enroll user and computer certificates automatically   | _   |
| <ul> <li>Do not enroll certificates automatically</li> <li>Enroll certificates automatically</li> </ul> |     |
| Renew expired certificates, update pending certificates, and remore<br>revoked certificates             | ove |
| Update certificates that use certificate templates  |     |
|   |     |
| OK Cancel App   | (y  |

16. **OK(확인)**를 클릭합니다.



<u>ACS용 내보내기 가능 인증서 구성</u>

**참고:** WLAN PEAP 클라이언트를 인증하려면 ACS 서버가 엔터프라이즈 루트 CA 서버에서 서버 인증서를 가져와야 합니다.

**참고:** 캐시된 정보에 문제가 발생하므로 인증서 설정 프로세스 중에 IIS 관리자가 열려 있지 않은지 확인하십시오.

- 1. 계정 관리 권한을 사용하여 ACS 서버에 로그인합니다.
- 2. System Administration(시스템 관리) > Configuration(컨피그레이션) > Local Server Certificates(로컬 서버 인증서)로 이동합니다. Add(추가)를 클릭합니다



 서버 인증서 생성 방법을 선택하는 경우 Generate Certificate Signing Request(인증서 서명 요 청 생성)를 선택합니다. Next(다음)를 클릭합니다



4. 인증서 제목과 키 길이를 예로 입력한 다음 Finish(마침)를 **클릭합니다**.인증서 주체 - **CN=acs.demo.local**키 길이 -

1024



5. ACS는 인증서 서명 요청이 생성되었음을 확인합니다. OK(확인)를 클릭합니다



6. System Administration(시스템 관리)에서 Configuration(**컨피그레이션) > Local Server Certificates(로컬 서버 인증서) >** Outstanding Signing Requests(**해결되지 않은 서명 요청)로 이동합니다.참고:** 이 단계를 수행하는 이유는 Windows 2003에서 내보낼 수 있는 키를 허용하 지 않으므로 앞서 생성한 ACS 인증서를 기반으로 인증서 요청을 생성해야 하기 때문입니다



7. Certificate Signing Request(인증서 서명 요청) 항목을 선택하고 Export(내보내기)를 클릭합니다



8. ACS certificate.**pem 파일**을 데스크톱에 저장합니다

| Save As   |                             |               |      |       | ? X    |
|---|-----------------------------|---------------|------|-------|--------|
| Save in:  | Desktop                     |               | . 00 | • 🖬 💙 |        |
| My Recent<br>Documents<br>Desktop<br>My Documents<br>My Documents | My Documents<br>My Computer | aces          |      |       |        |
| My Network  | File name:                  | ACS_ctd       |      | •     | Save   |
| Places  | Save as type:               | .pem Document |      | -     | Cancel |

### ACS 5.1 소프트웨어에 인증서 설치

다음 단계를 수행합니다.

1. 브라우저를 열고 CA 서버 URL http://10.0.10.10/certsrv에 연결합니다



2. Microsoft Certificate Services 창이 나타납니다. Request a certificate(인증서 요청)를 선택합



니다.

Microsoft Certificate Services - ca.demo.local

#### Request a Certificate

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

- 3. 고급 인증서 요청을 제출하려면 클릭합니다.
- 4. 고급 요청에서 Submit a certificate request using a base-64-encoded...(base-64로 인코딩된 인증서를 사용하여 인증서 요청 제출..)을 클릭합니다



5. 브라우저 보안이 허용되는 경우 Saved Request(저장된 요청) 필드에서 이전 ACS 인증서 요 청 파일을 찾아 삽입합니다

| Microsoft Certific  | ate Services - ca.demo.local Ho  | me |
|---|--|----|
| Submit a Certi  | ficate Request or Renewal Request  |    |
| To submit a sav<br>#10 certificate r<br>source (such as                       | red request to the CA, paste a base-64-encoded CMC or PKCS<br>request or PKCS #7 renewal request generated by an external<br>a Web server) in the Saved Request box. |    |
| Saved Request:  |  |    |
| Base-64-encoded<br>certificate request<br>(CMC or<br>PKCS #10 or<br>PKCS #7): | T<br>Browse for a file to insert.  |    |
| Certificate Templ   | late:  |    |
|   | Administrator  |    |
| Additional Attribu  | ites:  |    |
| Attributes:   | N N N N N N N N N N N N N N N N N N N  |    |
|   | Submit >   |    |

.

6. 브라우저의 보안 설정으로는 디스크의 파일에 액세스할 수 없습니다. 이 경우 확인을 **클릭하** 여 수동 붙여넣기를 수행합니다

| Windows | Internet Explorer   |
|---------|---|
| ♪       | Your web browser security settings prohibit this page from accessing your disk.<br>Either paste the data into this page manually, or add this page to your browser's list of trusted sites. |
|         | ОК  |

7. 이전 ACS 내보내기에서 ACS \*.pem 파일을 찾습니다. 텍스트 편집기(예: 메모장)를 사용하여



파일을 엽니다.

8. 파일의 전체 내용을 강조 표시하고 [**복사**]를 클릭합니다

| 📕 ACS_csr - Notepad   |        |
|-----------------------|--------|
| File Edit Format View | v Help |
| BEGIN CERT            | Undo   |
|                       | Cut    |
|                       | Сору   |

9. Microsoft 인증서 요청 창으로 돌아갑니다. **복사한** 내용을 Saved Request(저장된 요청) 필드

| To submit a say     | ved requ    | lest to the | CA      |
|---------------------|-------------|-------------|---------|
| renewal reques      | t genera    | ited by an  | exte    |
|                     | -           |             |         |
| Saved Request:      | 6           |             |         |
| Rass 64 anoddd      |             |             |         |
| certificate request |             | Undo        |         |
| (CMC or             |             | Cut         |         |
| PKCS #10 or         |             | Сору        |         |
| PKCS #7):           |             | Paste       |         |
|                     |             | Delete      | -       |
|                     | Destruction |             | and and |

10. ACS를 Certificate Template(인증서 템플릿)으로 선택하고 Submit(제출)을 클릭합니다

| Saved Request:  |   |
|---|---|
| Base-64-encoded<br>certificate request<br>(CMC or<br>PKCS #10 or<br>PKCS #7): | YIZIAYb4QgEBBAQDAgZAMAOGCSqGSIb3DQEBBQUA<br>DXoioRABct447w077+uAk8crn26oaEhcfG/ZR15X<br>ONZQ5xnrK23yxEdQNvSFC30mzRZEbQq4s5MvPE22<br>/MWqXej3NjpicpAgiV8CSwNd<br>END CERTIFICATE REQUEST |
| Certificate Temp  | late:   |
|   | ACS   |
| Additional Attribu  | utes:   |
| Attributes:   | ×<br>×  |
|   | Submit >  |

11. Certificate(인증서)가 발급되면 Base 64 encoded(Base 64 인코딩)를 선택하고 Download certificate(인증서 다운로드)를 클릭합니다

| Microsoft Certificate Services ca.demo.local   |
|--|
| Certificate Issued   |
| The certificate you requested was issued to you.   |
| C DER encoded or <a>Base 64 encoded</a>  |
| Download certificate chain   |
|  |
| File Download - Security Warning   |
| Do you want to open or save this file?   |
| Name: certnew.cer<br>Tupe: Security Certificate, 1.89KB  |
| Fion: ca   |
| Open Save Cancel   |
| While files from the Internet can be useful, this file type can<br>potentially harm your computer. If you do not trust the source, do not<br>open or save this software. What's the trisk? |

12. 인증서를 데스크톱에 저장하려면 Save(저장)를 클릭합니다



13. ACS > System Administration > Configuration > Local Server Certificates로 이동합니다. Bind CA Signed Certificate(CA 서명 인증서 바인딩)를 선택하고 Next(다음)를 클릭합니다



14. Browse(**찾아보기**)를 클릭하고 저장된 인증서를 찾습니다

| <ul> <li>Select server certificate creation method</li> </ul>  | Bind CA Signed Certificate  |
|--|---|
| Step 2 -Bind CA Signed Certif  | icate   |
| <ul> <li>Certificate File:</li> </ul>  | Browse  |
| Protocol   |   |
| EAP: Used for EAP protocols that use St  | SL/TLS tunneling  |
| Management Interface: Used to authenti   | cate the web server (GUI)   |
| Override Policy  |   |
| A certificate being imported may be determin<br>Subject or Issuer and serial number as an e<br>"Replace Certificate" option will allow the cer<br>existing protocol selections for the certificate | ed to already exist in ACS when it has either the same<br>xisting certificate. In such a case, selection of the<br>tificate contents to be replaced while retaining the . |
| Replace Certificate  |   |

15. CA 서버에서 발급한 ACS 인증서를 선택하고 Open(열기)을 **클릭합니다** 

| Choose file                                       |  |                              |   |         | <u>?×</u>      |
|---|--|------------------------------|---|---------|----------------|
| Look in   | Desktop  |                              | • | + 🖻 💣 🖬 |                |
| My Recent<br>Documents<br>Desktop<br>My Documents | My Documents<br>My Computer<br>My Network Place<br>ACS_cert<br>ACS_csr | 285                          |   |         |                |
| My Computer<br>My Network<br>Places               | File name:<br>Files of type:   | ACS, cert<br>All Files (".") |   | •       | Open<br>Cancel |

16. 또한 EAP의 Protocol(프로토콜) 상자를 **선택하고** Finish(마침)를 **클릭합니다** 



17. CA 발급 ACS 인증서가 ACS 로컬 인증서에 나타납니다

| System Administration > Configuration > Local Server Certificates > Local Certificates |                        |   |                |               |                  |  |
|--|------------------------|---|----------------|---------------|------------------|--|
| Local Certificates Showing 1-2 of 2 50 💌   |                        |   |                |               |                  |  |
| Filter   | Filter: Match if: Go 🔻 |   |                |               |                  |  |
|  | Friendly Name          | • | Issued To      | Issued By     | Valid From       |  |
|  | acs                    |   | acs            | acs           | 04:29 20.09.2010 |  |
|  | acs.demo.local         |   | acs.demo.local | ca.demo.local | 10:39 22:09:2010 |  |

<u>Active Directory에 대한 ACS ID 저장소 구성</u>

다음 단계를 수행합니다.

- 1. ACS에 연결하고 관리자 계정으로 로그인합니다.
- 2. Users and Identity Stores(사용자 및 ID 저장소) > External Identity Stores(외부 ID 저장소) >



#### Active Directory로 이동합니다.

3. Active Directory 도메인 *demo.local*을 입력하고 서버의 암호를 입력한 다음 **Test Connection(연결 테스트)**을 클릭합니다. 계속하려면 **OK**(확인)를 클릭합니다

| General   | Directory Groups  | Directory Attributes  |
|---|---|---|
| Connecti  | on Details  | -   |
| Active D<br>Name:   | irectory Domain   | demo.local  |
| Please sp   | ecify the credential  | s used to join this machine to the Active Directory Domain:   |
| o Userna  | me:   | administrator   |
| o Passw   | ord   |   |
| You may u<br>reachable  | use the Test Conne  | ction Button to ensure credentials are correct and Active Directory Doma Test Connection  |
| You may t<br>reachable<br>Click on 'S<br>have succ  | use the Test Conne<br>Save Changes' to c<br>ressfully connected   | ction Button to ensure credentials are correct and Active Directory Doma<br>Test Connection<br>onnect to the Active Directory Domain and save this configuration. Once y<br>to the Domain, yt Windows Internet Explorer   |
| You may t<br>reachable<br>Click on 'S<br>have succ<br>to be avail                               | use the Test Conne<br>Save Changes' to c<br>ressfully connected<br>lable for use in poli  | ction Button to ensure credentials are correct and Active Directory Doma<br>Test Connection<br>onnect to the Active Directory Domain and save this configuration. Once y<br>to the Domain, yt Windows Internet Explorer<br>cy rules.  |
| You may t<br>reachable<br>Click on 'S<br>have succ<br>to be avail<br>End User                   | use the Test Conne<br>Save Changes' to c<br>sessfully connected<br>lable for use in poli  | ction Button to ensure credentials are correct and Active Directory Doma Test Connection Test Connection To the Active Directory Domain and save this configuration. Once y to the Domain, yr Windows Internet Explorer (x) bu Connection test to 'demo.local' succeeded. ttings        |
| You may u<br>reachable<br>Click on 'S<br>have succ<br>to be avail<br>End User<br>I En:          | use the Test Conne<br>Save Changes' to c<br>ressfully connected<br>lable for use in poli<br>r Authentication Se<br>able password cha      | ction Button to ensure credentials are correct and Active Directory Doma Test Connection onnect to the Active Directory Domain and save this configuration. Once y to the Domain, y Windows Internet Explorer cy rules. Connection test to 'demo.local' succeeded. ttings nge CK        |
| You may t<br>reachable<br>Click on 'S<br>have succ<br>to be avail<br>End User<br>I En:<br>I En: | use the Test Conne<br>Save Changes' to c<br>ressfully connected<br>lable for use in poli<br><b>Authentication Se</b><br>able password cha | ction Button to ensure credentials are correct and Active Directory Doma Test Connection Test Connection To the Active Directory Domain and save this configuration. Once y to the Domain, yr Windows Internet Explorer (x) bu Connection test to 'demo.local' succeeded. CK entication |

4. Save Changes(변경 사항 저장)를 클릭합니다



**참고:** ACS 5.x 통합 절차에

대한 자세한 내용은 ACS <u>5.x 이상: Microsoft Active Directory Configuration Example과의 통</u> <u>합을</u> 참조하십시오.

#### ACS에 AAA 클라이언트로 컨트롤러 추가

다음 단계를 수행합니다.

1. ACS에 연결하고 Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)로 이동합니다. Create(생성)를 클릭합니다



2. 다음 필드에 을 입력합니다.이름 - wiciP - 10.0.1.10RADIUS 확인란 - 선택됨공유 암호 -

| o Name: wic   |                  |   |   |
|---|------------------|---|---|
| Description:  |                  |   |   |
| Network Device Grou                                 | ps               |   | -   |
| Location  | All Locations    |   | Select  |
| Device Type   | All Device Types |   | Select  |
| IP Address<br>Single IP<br>Address<br>IP: 10.0.1.10 | (s)              | Authentication Options<br>TACACS+<br>Shared Secret:<br>Single Connect Device<br>C Legacy TACACS+ Sin<br>TACACS+ Draft Comp<br>Support<br>RADIUS<br>NACACS+ Draft Comp<br>Support<br>C TACACS+ Draft Comp<br>Support<br>Use Device ID for Trust<br>Device ID:<br>Password: | e<br>gle Connect Suppo<br>bliant Single Conne<br>Sec identification |
|   |                  | TrustSec Advanced Set   | tings   |
| • = Required fields                                 |                  |   |   |

3. 완료되면 Submit(제출)을 클릭합니다. 컨트롤러가 ACS Network Devices(ACS 네트워크 디바이스) 목록에 항목으로 나타납니다

| ► 🛠 My Workspace  | Network | Resources  | s > Ne | twork Devices an | d AAA Clients |                |      |
|---|---------|------------|--------|------------------|---------------|----------------|------|
| Network Resources   | Netw    | vork Devic | es     |                  |               | Showing 1-1    | of 1 |
| <ul> <li>Network Device Groups<br/>Network Devices and AAA Clients</li> </ul> | Filte   | r. 🗌       |        | Match            | n it:         | 💌 Go 💌         |      |
| Default Network Device<br>External RADIUS Servers                             |         | Name       | •      | IP / Mask        | NDG:Location  | NDG:Device T   | Гуре |
| B Users and Identity Stores   |         | wic        |        | 10.0.1.10/32     | All Locations | All Device Typ | es   |
| Policy Elements   |         |            |        |                  |               |                |      |
| Access Policies   |         |            |        |                  |               |                |      |
| <ul> <li>Monitoring and Reports</li> </ul>                                    |         |            |        |                  |               |                |      |

### <u>무선에 대한 ACS 액세스 정책 구성</u>

다음 단계를 수행합니다.

1. ACS에서 Access Policies(액세스 정책) > Access Services(액세스 서비스)로 이동합니다



2. Access Services(액세스 서비스) 창에서 Create(생성)를 클릭합니다

| Access P | olicies > Access Services |                       |                           |              |
|----------|---------------------------|-----------------------|---------------------------|--------------|
| Acces    | s Services                |                       | Showing 1-2 of 2          | 50 💌 per p   |
| Filter:  | Match i                   | t                     | Go 🔻                      |              |
|          | Name 🔺                    | Service Type          | Included Policies         | Description  |
|          | Default Device Admin      | Device Administration | Identity<br>Authorization | Default Devi |
|          | Default Network Access    | Network Access        | Identity<br>Authorization | Default Netw |
| -        |                           |                       |                           | 1            |
| Crea     | te Duplicate Edit         | Delete                | Page                      | 1 of 1       |

3. 액세스 서비스를 생성하고 이름(예: WirelessAD)을 입력합니다. Based on **service template(서** 

비스 템플릿 기반)을 선택하고 Select(선택)를 클릭합니다

.

| Access Policies > Access Services > Create  |        |
|---|--------|
| General Allowed Protocols                   |        |
| Step 1 - General                            |        |
| General                                     |        |
| Name: WirelessAD                            |        |
| Description:                                |        |
| Access Service Policy Structure             |        |
| Based on service template                   | Select |
| O Based on existing service                 | Select |
| O User Selected Service Type Network Access |        |
|   |        |

4. 웹 페이지 대화 상자에서 Network Access - Simple을 선택합니다. OK(확인)를 클릭합니다

| Acces   | s Services                                 |                       | Showing 1-4 |
|---------|--|-----------------------|-------------|
| Filter: | Match if:                                  | Go 🗢                  |             |
|         | Name 🔺                                     | Service Type          | Description |
| 0       | Device Admin - Command Auth                | Device Administration |             |
| C       | Device Admin - Simple                      | Device Administration |             |
| 0       | Network Access - MAC Authentication Bypass | Network Access        |             |
| •       | Network Access - Simple                    | Network Access        |             |

5. 웹 페이지 대화 상자에서 Network Access - Simple을 선택합니다. OK(확인)를 클릭합니다. 템 플릿이 선택되면 다음을 클릭합니다

| Step 1 - General                                  |        |
|---|--------|
| General   |        |
| Name: WirelessAD                                  |        |
| Description:                                      |        |
| Access Service Policy Structure                   |        |
| Based on service template Network Access - Simple | Select |
| C Based on existing service                       | Select |
| C User Selected Service Type Network Access       |        |

6. Allowed Protocols(허용된 프로토콜)에서 Allow MS-CHAPv2(MS-CHAPv2 허용) 및 Allow PEAP(PEAP 허용)의 확인란을 선택합니다. Finish(마침)를 클릭합니다



7. ACS에서 새 서비스를 활성화하라는 메시지가 표시되면 Yes(예)를 클릭합니다



8. 방금 생성/활성화된 새 액세스 서비스에서 Identity(ID)를 확장하고 **선택합니다**. Identity Source(ID 소스)에서 Select(**선택)**를 클릭합니다



9. ACS에 구성된 Active Directory에 대해 AD1을 선택하고 OK(확인)를 클릭합니다

| ¢ | Cisco Secure ACS Webpage Dialog |                |   |  |  |  |  |
|---|---------------------------------|----------------|---|--|--|--|--|
|   | Identity Store                  |                |   |  |  |  |  |
|   | Filter:                         |                | Match if: Go 🔻                                |  |  |  |  |
|   |                                 | Name 🔺         | Description                                   |  |  |  |  |
|   | C                               | AD1            |   |  |  |  |  |
|   | 0                               | CN Username    | Predefined Certificate Authentication Profile |  |  |  |  |
|   | 0                               | DenyAccess     |   |  |  |  |  |
|   | 0                               | Internal Hosts |   |  |  |  |  |
|   | 0                               | Internal Users |   |  |  |  |  |
|   | 0                               | NAC Profiler   | Default Entry for NAC Profiler                |  |  |  |  |
|   |                                 |                |   |  |  |  |  |

10. ID 소스가 AD1인지 확인하고 Save Changes(변경 사항 저장)를 클릭합니다



### <u>ACS 액세스 정책 및 서비스 규칙 생성</u>

다음 단계를 수행합니다.

1. Access Policies(액세스 정책) > Service Selection Rules(서비스 선택 규칙)로 이동합니다



2. Service **Selection** Policy(서비스 선택 정책) 창에서 Create(생성)를 클릭합니다. 새 규칙에 이 름을 지정합니다(예: *WirelessRule*). Protocol to match Radius(Radius와 일치하는 **프로토콜**)에 대한 확인란**을 선택합니다** 

| 🖉 Cisco Secure ACS Webpage Dialo            | g               |                              |                        |                        |                       |
|---|-----------------|------------------------------|------------------------|------------------------|-----------------------|
| General<br>Name: WirelessRule               | Status:         | Enabled                      | • •                    |                        |                       |
| The Customize button conditions and results | in the<br>are a | lower right<br>vailable here | area of t<br>e for use | he policy<br>in policy | rules scree<br>rules. |
| Conditions                                  |                 |                              |                        |                        |                       |
| Protocol: match                             | •               |                              |                        |                        | Select                |
| Results                                     |                 |                              |                        |                        |                       |
|   | Cisco           | Secure ACS \                 | Webpage Di             |                        |                       |
|   | Enum            | Definition                   |                        |                        |                       |
|   |                 | Enum Name                    | ID                     |                        |                       |
|   | C               | Radius                       | 0                      |                        |                       |

Tacacs

1

- 3. Radius를 선택하고 OK를 클릭합니다.
- 4. Results(결과)에서 **WirelessAD** for Service (created in previous step)(서비스용 WirelessAD(이전 단계에서 생성됨))를 선택합니다

|                     | esuits are available here for | use in policy rules |
|---------------------|-------------------------------|---------------------|
| Conditions          |                               |                     |
| Protocol: match     | Radius                        | Sele                |
| Results             |                               |                     |
| Service: WirelessAD |                               |                     |

5. 새 무선 규칙이 생성되면 이 규칙을 선택하고 맨 위로 **이동합니다.** 이 규칙은 Active Directory를 사용하여 무선 RADIUS 인증을 식별하는 첫 번째 규칙이 됩니다

| Sen  | Service Selection Policy |         |                  |                   |                       |  |  |
|------|--------------------------|---------|------------------|-------------------|-----------------------|--|--|
| Filb | er: Sta                  | atus 🔄  | Match if: Equ    | als 💌             | Clear                 |  |  |
|      |                          | Status  | Name             | Protocol          | Conditions            |  |  |
| 3    |                          | •       | WirelessRule     | match Radius      |                       |  |  |
| 1    |                          | 0       | Rule-1           | match Radius      |                       |  |  |
| 2    |                          | 0       | Rule-2           | match Tacacs      |                       |  |  |
|      |                          |         |                  |                   |                       |  |  |
|      |                          |         |                  |                   |                       |  |  |
| •[   |                          |         |                  |                   |                       |  |  |
| ••   | Г                        | Default |                  | If no rules defin | ed or no enabled rule |  |  |
| Cr   | reate                    | I- D    | uplicate   -   E | dit Delete        | Move to V             |  |  |

# <u>Windows Zero Touch를 사용하는 PEAP에 대한 클라이언트 구성</u>

이 예에서 CLIENT는 Windows XP Professional with SP를 실행하는 컴퓨터로, 무선 클라이언트 역 할을 하며 무선 AP를 통해 인트라넷 리소스에 대한 액세스를 얻습니다. CLIENT를 무선 클라이언트 로 구성하려면 이 섹션의 절차를 완료합니다.

### <u>기본 설치 및 구성 수행</u>

다음 단계를 수행합니다.

- 1. 허브에 연결된 이더넷 케이블을 사용하여 CLIENT를 인트라넷 네트워크 세그먼트에 연결합니 다.
- 2. CLIENT에서 Windows XP Professional(SP2 포함)을 demo.local 도메인의 CLIENT라는 구성 원 컴퓨터로 설치합니다.

3. Windows XP Professional을 SP2와 함께 설치합니다. PEAP를 지원하려면 설치해야 합니다 .**참고:** Windows 방화벽은 Windows XP Professional with SP2에서 자동으로 설정됩니다. 방화 벽을 끄지 마십시오.

<u>무선 네트워크 어댑터 설치</u>

다음 단계를 수행합니다.

- 1. 클라이언트 컴퓨터를 종료합니다.
- 2. 인트라넷 네트워크 세그먼트에서 클라이언트 컴퓨터의 연결을 끊습니다.
- 3. 클라이언트 컴퓨터를 다시 시작한 다음 로컬 관리자 계정을 사용하여 로그온합니다.
- 4. 무선 네트워크 어댑터를 설치합니다.**참고:** 무선 어댑터용 제조업체의 구성 소프트웨어를 설치 하지 마십시오. 하드웨어 추가 마법사를 사용하여 무선 네트워크 어댑터 드라이버를 설치합니 다. 또한 메시지가 표시되면 제조업체가 제공한 CD나 Windows XP Professional with SP2에 사용할 업데이트된 드라이버가 포함된 디스크를 제공합니다.

### <u>무선 네트워크 연결 구성</u>

다음 단계를 수행합니다.

- 1. demo.local 도메인의 WirelessUser 계정을 사용하여 로그오프한 다음 로그인합니다.
- 시작 > 제어판을 선택하고 네트워크 연결을 두 번 클릭한 다음 무선 네트워크 연결을 마우스 오른쪽 단추로 클릭합니다.
- 3. 속성을 클릭하고 무선 네트워크 탭으로 이동한 다음 Windows를 사용하여 내 무선 네트워크

| Wireless Network Connection Pr   | operties  | ? |
|--|---|---|
| General Wireless Networks Advan  | ced   |   |
| Use Windows to configure my wir  | eless network settings                              |   |
| - Available network e  |   | _ |
| To connect to, disconnect from, or<br>about wireless networks in range, or | find out more information<br>lick the button below. |   |
|  | View Wireless Networks                              | 1 |
|  | Move up<br>Move down                                | ] |
| Add Remain   | Properties  |   |
| Learn about setting up wireless netw                                       | vork Advanced                                       | 1 |
| Learn about <u>setting up wireless network</u>                             | Model Caro  | ] |

**설정을 구성하는지** 확인합니다.

- 4. Add(추가)를 클릭합니다.
- 5. Association(연결) 탭 아래의 Network name(SSID) 필드에 Employee(직원)를 입력합니다.

6. 네트워크 인증에 대해 WPA를 선택하고 데이터 암호화가 TKIP로 설정되어 있는지 확인합니

| Association Authentication                             | Connection                  |             |
|--|-----------------------------|-------------|
| Network name (SSID):                                   | Employee                    |             |
| Wireless network key                                   |                             |             |
| This network requires a key                            | for the following:          |             |
| Network Authentication:                                | WPA                         |             |
| Data encryption:                                       | TKIP                        | -           |
| Network key:   |                             |             |
| Confirm network key:                                   |                             |             |
| Key index (advanced):                                  | 1                           |             |
| The key is provided for                                | me automatically            |             |
| This is a computer-to-com<br>access points are not use | puter (ad hoc) network<br>d | ;; wireless |

- 7. Authentication(**인증)** 탭을 클릭합니다.
- 8. EAP 유형이 PEAP(Protected EAP)를 사용하도록 **구성되었는지 확인합니다**. 그렇지 않은 경 우 드롭다운 메뉴에서 선택합니다.
- 9. 로그인 전에 시스템을 인증하여 로그인 스크립트 또는 그룹 정책 푸시를 적용할 수 있도록 하 려면 **컴퓨터 정보**를 사용할 **수 있는 경우 컴퓨터로 인증을 선택합니다**

| Wireless network properties |   |             |               |  |      |
|-----------------------------|---|-------------|---------------|--|------|
| Association                 | Authentication  | Connecti    | on            |  |      |
| Select this<br>wireless Et  | option to provide<br>ternet networks.                         | authentica  | ited network  | access for                             |      |
| 💌 Enable                    | IEEE 802.1x auth  | hentication | for this netw | ork                                    |      |
| EAP type:                   | Protected EAP   | (PEAP)      |               |  | •    |
| Authen<br>availab           | ticate as <u>c</u> ompute<br>le<br>ticate as guest wi<br>able | er when co  | mputer inform | Propertie<br>nation is<br>formation is | :5   |
|                             |   | [           | OK            | Car                                    | ncel |

- 10. 속성을 **클릭합니다**.
- 11. PEAP는 클라이언트에 의한 서버 인증을 포함하므로 Validate **server certificate(서버 인증서 검증)**가 선택되었는지 확인합니다. 또한 ACS 인증서를 발급한 CA가 Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) 메뉴에서 선택되어 있는지 확인합니 다.
- 12. 내부 인증**에** 사용 **하므로 인증 방법**에서 보안 암호 **(EAP-**MSCHAP v**2**)를 선택 합니다

| Protected EAP Properties   |
|--|
| When connecting:   |
| Validate server certificate  |
| Connect to these servers:  |
| Trusted Root Certification Authorities:  |
| C&W HKT SecureNet CA Root CA 1 Ca.demo.local Certiposte Classe A Personne Certiposte Serveur Certisign - Autoridade Certificadora - AC2 Certisign - Autoridade Certificadora - AC4 |
| Do not prompt user to authorize new servers or trusted certification authorities.  |
| Select Authentication Method:  |
| Secured password (EAP-MSCHAP v2)   |
| Enable Fast Reconnect  |
| OK Cancel  |

- 13. 빠른 재연결 **사용 확인란**이 선택되었는지 확인합니다. 그런 다음 확인을 세 번 **클릭합니다**.
- 14. Systray에서 무선 네트워크 연결 아이콘을 마우스 오른쪽 단추로 클릭한 다음 사용 가능한 무 선 네트워크 보기를 클릭합니다.
- 15. 직원 무선 네트워크를 클릭한 다음 연결을 **클릭합니다**. 연결이 성공하면 무선 **클라이언트**에 Connected(연결됨)가 표시됩니다



- 16. 인증에 성공하면 네트워크 연결을 사용하여 무선 어댑터에 대한 TCP/IP 컨피그레이션을 확 인합니다. DHCP 범위 또는 CorpNet 무선 클라이언트에 대해 생성된 범위에서 주소 범위가 10.0.20.100-10.0.20.200이어야 합니다.
- 17. 기능을 테스트하려면 브라우저를 열고 http://10.0.10.10(**또는** CA 서버의 IP 주소)로 이동합 니다.

# <u>ACS로 무선 인증 문제 해결</u>

다음 단계를 수행합니다.

1. ACS > Monitoring and Reports로 이동하여 Launch Monitoring & Report Viewer를 클릭합니다



2. 별도의 ACS 창이 열립니다. Dashboard를 클릭합니다



3. My Favorite Reports(내 즐겨찾기 보고서) 섹션에서 Authentications - RADIUS - Today(인증 - RADIUS - 오늘)를 클릭합니다

| ly Favorite Reports               |  |  |  |  |
|-----------------------------------|--|--|--|--|
| Favorite Name                     | Report Name                            |  |  |  |
| ACS - Configuration Audit - Today | ACS Instance>ACS_Configuration_Audi    |  |  |  |
| ACS - System Errors - Today       | ACS<br>Instance>ACS_System_Diagnostics |  |  |  |
| Authentications - RADIUS - Today  | AAA Protocol>RADIUS_Authentication     |  |  |  |

4. 로그에 모든 RADIUS 인증이 Pass(통과) 또는 Fail(실패)로 표시됩니다. 로깅된 항목 내에서 Details(세부사항) 열에서 **돋보기 아이콘**을 클릭합니다

| AAA Protocol > RADI   | JS Authenticati                                | on        |                   |                     |            |                     |  |
|---|--|-----------|-------------------|---------------------|------------|---------------------|--|
| Authentication Status : Pass or Fail<br>Date : September 22, 2010 (Last 30 Minutes   Last Hour   Last 12 Hours   Today   Yesterday   Last 7 Days   Last 30 Days ) |  |           |                   |                     |            |                     |  |
| Generated on September  | Generated on September 22, 2010 5:51:34 PM PDT |           |                   |                     |            |                     |  |
| @Reload   |  |           |                   |                     |            |                     |  |
| ✓=Pass ×=Fail 🍳   | Click for details                              | R = Mouse | over item for add | itional information |            |                     |  |
| Logged At RADIUS NAS<br>Status Failure Details Username MAC/IP<br>Address Access Service Authentication<br>Method   |  |           |                   |                     |            |                     |  |
| Sep 22,10 5:51:17.843 F   | M 🖌  | 9         | wirelessuser      | 00-21-5c-69-9a-39   | WirelessAD | PEAP (EAP-MSCHAPv2) |  |

5. RADIUS Authentication Detail(RADIUS 인증 세부사항)은 로깅된 시도에 대한 많은 정보를 제

| AAA Protocol > RADIUS Authentication Detail                   |  |  |  |  |  |
|---|--|--|--|--|--|
| ACS session ID : acs/74551189/31<br>Date : September 22, 2010 |  |  |  |  |  |
| Generated on September 22, 2010 5:52:16 PM PDT                |  |  |  |  |  |
| ary   |  |  |  |  |  |
| September 22,2010 5:51:17.843 PM                              |  |  |  |  |  |
| Authentication succeeded                                      |  |  |  |  |  |
|   |  |  |  |  |  |
| wirelessuser  |  |  |  |  |  |
| 00-21-5c-69-9a-39   |  |  |  |  |  |
| wlc : 10.0.1.10 :   |  |  |  |  |  |
| WirelessAD  |  |  |  |  |  |
| AD1   |  |  |  |  |  |
| Permit Access   |  |  |  |  |  |
|   |  |  |  |  |  |
| PEAP(EAP-MSCHAPv2)  |  |  |  |  |  |
|   |  |  |  |  |  |
6. ACS 서비스 적중 횟수는 ACS에서 생성된 규칙과 일치하는 시도의 개요를 제공할 수 있습니 다. ACS > Access Policies > Access Services로 이동하고 Service Selection Rules를 클릭합

| Results<br>Service     | Hit Count |
|------------------------|-----------|
| WirelessAD             | 33        |
| Default Network Access | 0         |

## ACS 서버에서 PEAP 인증 실패

클라이언트가 ACS 서버를 사용한 PEAP 인증에 실패하면 ACS의 **Report and Activity** 메뉴 아래의 Failed attempts(실패한 시도) 옵션에서 NAS duplicated authentication attempt(NAS 오류) 메시지 를 찾는지 확인합니다.

Microsoft Windows XP SP2가 클라이언트 시스템에 설치되고 Windows XP SP2가 Microsoft IAS 서버가 아닌 타사 서버에 대해 인증될 때 이 오류 메시지가 표시될 수 있습니다. 특히 Cisco RADIUS 서버(ACS)는 Windows XP에서 사용하는 방법과 다른 방법으로 EAP-TLV(Extensible Authentication Protocol Type:Length:Value Format) ID를 계산합니다. Microsoft에서는 이 문제가 XP SP2 서플리컨트의 결함이라고 확인했습니다.

핫픽스의 경우 Microsoft에 문의하고 타사 RADIUS 서버에 <u>연결할 때 PEAP 인증에 성공하지 못함</u> <u>문서를 참조하십시오</u>. 기본적인 문제는 Windows 유틸리티의 클라이언트 측에서 빠른 재연결 옵션 이 기본적으로 PEAP에 대해 비활성화되어 있다는 것입니다. 그러나 이 옵션은 기본적으로 서버 측 (ACS)에서 활성화되어 있습니다. 이 문제를 해결하려면 ACS 서버의 Global System Options(전역 시스템 옵션) 아래에서 Fast Reconnect(빠른 재연결) 옵션의 선택을 취소합니다. 또는 클라이언트 측에서 빠른 재연결 옵션을 활성화하여 문제를 해결할 수 있습니다.

Windows 유틸리티를 사용하여 Windows XP를 실행하는 클라이언트에서 빠른 재연결을 활성화하 려면 다음 단계를 수행합니다.

- 1. 시작 > 설정 > 제어판으로 이동합니다.
- 2. Network Connections(네트워크 연결) 아이콘을 두 번 클릭합니다.
- 3. **무선 네트워크 연결** 아이콘 을 마우스 오른쪽 단추로 클릭한 다음 속성 을 **클릭합니다**.
- 4. Wireless Networks(무선 네트워크) 탭을 클릭합니다.
- 5. Windows에서 **클라이언트 어댑터를 구성할 수 있도록 하려면 Windows**를 사용하여 내 **무선 네 트워크** 설정을 구성합니다 옵션을 선택합니다.
- 6. SSID를 이미 구성한 경우 SSID를 선택하고 Properties(속성)를 **클릭합니다**. 그렇지 않은 경우 New(새로 만들기)를 클릭하여 새 WLAN을 추가합니다.
- 7. Association(연결) 탭 아래에 SSID를 입력합니다. 네트워크 인증이 **열려** 있고 데이터 암호화가 WEP로 설정되어 있는지 **확인합니다**.
- 8. Authentication(인증)을 클릭합니다.
- 9. Enable IEEE 802.1x authentication for this network 옵션을 선택합니다.
- 10. EAP 유형으로 PEAP를 선택하고 속성을 클릭합니다.
- 11. 페이지 하단에서 빠른 재연결 활성화 옵션을 선택합니다.

## <u>관련 정보</u>

- <u>ACS 4.0 및 Windows 2003을 사용하는 Unified Wireless Networks에서 PEAP</u>
- <u>웹 인증을 위한 Cisco WLC(Wireless LAN Controller) 및 Cisco ACS 5.x(TACACS+) 컨피그레 이션 예</u>
- <u>Cisco Secure Access Control System 5.1 설치 및 업그레이드 가이드</u>
- <u>기술 지원 및 문서 Cisco Systems</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.