# CAPF Online CA를 통한 자동 인증서 등록 및 갱 신 구성

목차	
<u>소개</u>	
<u>사전 요구 사항</u>	
<u>요구 사항</u>	
<u>사용되는 구성 요소</u>	
<u>배경 정보</u>	
<u>서버 시간 및 날짜 확인</u>	
<u>업데이트 서버 컴퓨터 이름</u>	
<u>구성</u>	
<u>AD 서비스, 사용자 및 인증서 템플릿</u>	
<u>IIS 인증 및 SSL 바인딩 구성</u>	
<u>CUCM 컨피그레이션</u>	
<u>다음을 확인합니다.</u>	
<u>IIS 인증서 확인</u>	
<u>CUCM 컨피그레이션 확인</u>	
<u>관련 링크</u>	

# 소개

이 문서에서는 CUCM(Cisco Unified Communications Manager)용 CAPF(Certificate Authority Proxy Function) Online 기능을 통한 자동 인증서 등록 및 갱신에 대해 설명합니다.

기고자: Michael Mendoza, Cisco TAC 엔지니어

# 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Communications Manager
- X.509 인증서
- Windows 서버
- Windows AD(Active Directory)
- Windows 인터넷 정보 서비스(IIS)
- NT(신기술) NTLM(LAN Manager) 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 버전 12.5.1.10000-22
- Windows Server 2012 R2
- IP Phone CP-8865 / 펌웨어: SIP 12-1-1SR1-4 및 12-5-1SR2.

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

이 문서에서는 추가 연구를 위한 기능 및 관련 리소스의 구성을 다룹니다.

서버 시간 및 날짜 확인

Windows 서버가 서버의 루트 CA(Certificate Authority) 인증서뿐만 아니라 서버에서 발급한 인증서 의 유효 시간에 영향을 미치므로 올바른 날짜, 시간 및 표준 시간대를 구성했는지 확인합니다.

업데이트 서버 컴퓨터 이름

기본적으로 서버의 컴퓨터 이름에는 WIN-730K65R6BSK와 같은 임의의 이름이 있습니다. AD 도메 인 서비스를 활성화하기 전에 먼저 서버의 컴퓨터 이름을 설치 종료 시까지 서버의 호스트 이름 및 루트 CA 발급자 이름으로 업데이트해야 합니다. 그렇지 않으면 AD 서비스를 설치한 후 이를 변경 하는 데 많은 추가 단계가 필요합니다.

- Local Server(로컬 서버)로 이동하여 Computer name(컴퓨터 이름)을 선택하여 System Properties(시스템 속성)를 엽니다
- 변경 단추를 선택하고 새 컴퓨터 이름을 입력합니다.

Server Manager •	Local Server	• ③   🏲 Manage Tools View Help
ege Services > Windows Fi Remote ma Remote Del NIC Teamin Ethernett) Coperating s Handware in C	ERTIES N-730KSSASSEX anne WN-730KSSASSEX Last in WORKSROUP View System Properties  Computer Name Hadware Advanced Penote  Computer Name Hadware Advanced Penote  Computer Secondate  Computer Secondate  Computer Secondate  Computer Secondate  Computer Name  Workgroup  Workgroup  Computer name  Workgroup  Workgroup  Computer name  Workgroup  Workgroup	Computer Name/Domain Changes       X         You can change the name and the membership of this computer changes might affect access to network resources.         Computer name:         LABOC RTP         Aid computer name:         LABOC RTP         More         Onmar:         Worksprag:         Worksprag:         OK
	V VESS 1997	Windows Server 2012 F

• 변경 내용을 적용하려면 서버를 다시 시작하십시오.

# 구성

AD 서비스, 사용자 및 인증서 템플릿

Active Directory 서비스 활성화 및 구성

 서버 관리자에서 [역할 및 기능 추가] 옵션을 선택하고 역할 기반 또는 기능 기반 설치를 선택 한 다음 풀에서 서버를 선택한 다음(풀에는 하나만 있어야 함) Active Directory 도메인 서비스 를 선택합니다.

5	Add Roles and Features Wiza	rd a x
Select se	rver roles	DESTANTION SERVER WIN-730KBR86K
Before You Installation	Select one or more roles to install on the selected a you Roles	Description X
Server Role	Active Directory Certificate Services     Active Directory Domain Services     Active Directory Federation Services     Active Directory Federation Services	Add Roles and Features Wizard
	Active Directory Rights Management Server Application Server DHCP Server	You cannot install Active Directory Domain Services the following with approximation of the process of the following with approximation of the process of th
	DNS Server      Pax Server      Rever      M File and Storage Services (1 of 12 installed      Myper-V      Network Policy and Access Services      Print and Document Services      Remote Access      Remote Desktop Services	[Tools] Group Policy Management     Remote Server Administration Tools     Role Administration Tools     AD DS and AD LDS Tools     Active Directory module for Windows PowerShell     AD DS Tools     [Tools] Active Directory Administrative Center     [Tools] Active Directory Administrative Center     [Tools] Active Directory Administrative Center
	K Previou BPA results Per	Include management tools (if applicable)

- 다음 단추를 계속 선택한 다음 설치
- 설치가 완료되면 닫기 단추를 선택합니다
- 서버 관리자 > AD DS 아래에 Active Directory 도메인 서비스에 필요한 구성 이라는 제목의 경고 탭이 나타납니다. 다른 링크를 선택한 다음 사용 가능한 작업을 선택하여 설치 마법사를 시 작합니다.

€ • Server M	anager • AD DS • ⓒ I 🌇 Menager tools Were Hole	
Dashboard     Local Server     At Servers     At Servers     AD 05	SDAVERS All servers   1 total Table A Configuration required for Active Directory Domain Services at WH-7304358665X block Fiber P ® T Configuration Fiber P ® T Configuration Fiber P ® T Configuration Fiber P P P P P P P P P P P P P P P P P P P	
II File and Storage Services ▶	All Servers Task Details	
	All Servers Task Details and Notifications	
	Par P (8 * (8 *	$\odot$
	C Status Task Name Stage Message Action	N
	Post-deployment Configuration Not Sta. Configuration required for Active Directory Do. <u>Econote this secret to a</u>	ulomain- 1

• 도메인 설정 마법사의 프롬프트에 따라 원하는 루트 도메인 이름(이 실습에 michamen.com 사용)을 사용하여 새 포리스트를 추가하고 사용 가능한 경우 DNS 확인란의 선택을 취소하고

DSRM 암호(이 실습에 C1sc0123 사용)를 정의합니다.

<b>b</b>	Active Directory Domain Services	Configuration Wizard	_ = X
Deployment Conf	iguration		TARGET SERVER
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check	Select the deployment operation Add a domain controller to an exist Add a new domain to an existing for Add a new forest Specify the domain information for this Root domain name:	ing domain rest operation michamen.com	
Domain Controlle	Active Directory Domain Services (	Configuration Wizard	TARGET SERVER
Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest Forest functional level: Domain functional level: Specify domain controller capabilities Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mod Password: Confirm password:	and root domain Windows Server 2012 R2 Windows Server 2012 R2 Se (DSRM) password	•

- NetBIOS 도메인 이름을 지정해야 합니다(이 실습에서 MICHAMEN1에 사용됨).
- 마법사를 따라 완료합니다. 그런 다음 서버가 재부팅되어 설치를 완료합니다.
- 다음에 로그인할 때 새 도메인 이름을 지정해야 합니다. 예: MICHAMEN1\Administrator.

€ - Server M	anager + AD DS		· @ I
III Dashboard Local Server III All Servers	Filter	• ۵ • ۵	
AD DS	Server Name IPv4 Address	Manageability	Last Update

#### 인증서 서비스 활성화 및 구성

- 서버 관리자에서 역할 및 기능 추가를 선택합니다
- Active Directory Certificate Services(Active Directory 인증서 서비스)를 선택하고 프롬프트에 따라 필요한 기능을 추가합니다(사용 가능한 모든 기능은 이 실습에 대해 활성화된 역할 서비 스에서 선택됨).
- Role Services의 경우 인증 기관 웹 등록 확인

<b>b</b>	Add Roles and Features Wizard	_ <b>_</b> X
Select role service	9S	DESTINATION SERVER LAB-DC-877.michamen.com
Before You Begin	Select the role services to install for Active Directory Certifi	icate Services
Installation Type	Role services	Description
Server Selection	A Cartification botherity	Certification Authority Web
Server Roles	Certificate Enrollment Policy Web Service	Enrollment provides a simple Web interface that allows users to
Features	Certificate Enrollment Web Service	perform tasks such as request and
AD CS	Certification Authority Web Enrolment	renew certificates, retrieve certificate
Role Services	Network Device Enrollment Service	smart card certificates.
Web Server Role (IIS)	Online Responder	
Role Services		
Confirmation		



• 경고 탭은 서버 관리자 >AD DS 아래에 Active Directory 인증서 서비스에 필요한 구성 이라는 제목으로 나타나야 합니다. more 링크를 선택한 다음 사용 가능한 작업을 선택하십시오.

€ • Server M	lanager + AD CS	i -		· @   🗛 🏎	Tools View 1	Huly	
Coshboard Local Server All Servers All Servers AD DS File and Storage Services	SERVERS A configuration require False Dense Name (Publisher DALOCATE (BARLE)	el for Active Directory Certificate (P) (8) • (1) 10 Manupathility 10 Online - Redenment (south	Services at LAB-DC-ATP B) • Last Tipology 1 Not always & 2010/2014 42110	Windpase Activation	too • too. •		
go IIS	EVENTS All events   2 total   Feber	All Servers Ta At Turk   1 total / Atr / Atr / Datus Task Name	sk Details and No P ® • Step &	All Servers Task Des otifications ® • Annage adaptation region for Anna 1	Alta Action Section Content	er Julius Directory Sert	Transfer

- AD-CS 설치 후 구성 마법사에서 다음 단계를 진행합니다.
- 인증 기관 및 인증 기관 웹 등록 역할 선택
- 옵션이 있는 Enterprise CA를 선택합니다.
- 루트 CA
- •새개인키만들기
- 개인 키 사용 SHA1(기본 설정 포함)

• CA의 Common Name(공통 이름)을 설정합니다(서버의 호스트 이름과 일치해야 함).

<u>1</u>	AD CS Configuration
CA Name	DESTINATION SERVER LA8-DC-RTRmichamen.com
Credentials Role Services Setup Type CA Type Private Key	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified. Common name for this CA:
Cryptography	LA8-DC-RTP
Validity Period Certificate Database Confirmation Progress Results	Distinguished name suffix: DC=michamen,DC=com Preview of distinguished name: CN=LA8-DC-RTP,DC=michamen,DC=com

- 5년(원하는 경우 이상)으로 유효 기간 설정
- 마법사의 나머지 부분에서 다음 단추를 선택합니다.

#### CiscoRA용 인증서 템플릿 생성

- MMC를 엽니다. Windows 시작 로고를 선택하고 실행에서 mmc를 입력합니다
- MMC 창을 열고 후속 스냅인(컨피그레이션의 다른 지점에서 사용됨)을 추가한 다음 OK(확인)를 선택합니다.

8						
in.	File	Action	View	Favorites	Window	Help
4		New			c	trl+N
12		Open			c	trl+O
4		Save			0	trl+S
		Save As				
1		Add/Rem	ove Sna	ip-in	C	rl+M
		Options				

ap-in	Vendor	~		Console Root	Edit Extensions
Active Directory Do Active Directory Site Active Directory Use	Microsoft Cor Microsoft Cor Microsoft Cor	=		Active Directory Domains and True Active Directory Users and Compu Certification Authority (Local)	Remove
ActiveX Control ADSLEdit	Microsoft Cor	_		Certificate Templates (LAB-DC.mic	Move Up
Authorization Manager Certificate Templates Certificates Certification Authority Component Services	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor		Add >		Move Down
Device Manager Disk Management DNS	Microsoft Cor Microsoft Cor Microsoft and Microsoft Cor	v		< III >	Advanced
cription:					

• File(파일) > Save(저장)를 선택하고 빠른 재액세스를 위해 이 콘솔 세션을 데스크톱에 저장합 니다.

- 스냅인에서 인증서 템플릿을 선택합니다
- 템플릿(사용 가능한 경우 "루트 인증 기관" 템플릿)을 생성하거나 복제하고 이름을 CiscoRA로 지정합니다

Con:	sole1 - [Console Root\Certificate Ter	mplates (LAB-DC-
🚟 File Action View Favorites Window Help		
Console Root  Console Root  Active Directory Domains and Trusts  Active Directory Users and Computers  Certification Authority (Local)	Template Display Name Administrator Authenticated Session Basic EFS	Schema Version 1 1
Certificate Templates LAB-DC-RTP.michamen.com)	CA Exchan Construction Construc	e Holders

- 템플릿을 수정합니다. 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
- 일반 탭을 선택하고 유효 기간을 20년(또는 원하는 경우 다른 값)으로 설정합니다. 이 탭에서 템플릿의 "표시 이름" 및 "이름" 값이 일치하는지 확인합니다

CiscoRA Properties ? X							
Subject Name Issuance Requirements							
Superseded Templates	s Edensions	Edensions Security Server					
General Compatibility	Request Handling	Cryptography	Key Attestation				
Template display name:							
CiscoRA							
Template name: CiscoRA Validity period: years v 10 days v							
Publish certificate in Do not automatic Directory	Active Directory ally reenrol if a dupli	cate certificate e	xists in Active				
OK	Cancel	Apply	Help				

• Extensions(확장) 탭을 선택하고 Application Policies(애플리케이션 정책)를 선택한 다음 Edit(수정)를 선택합니다

<b>6</b>	Console1	- [Console Root\Cer	tificate Templ	ates (LAB-D	C-RTP.micham
<ul> <li>File Action View Favorites Window H</li> <li>File Action View Favorites Window H</li> <li>File Active Directory Domains and Trusts</li> <li>Active Directory Users and Computers</li> </ul>	Template Displ	Console Koot\Cer     Subject Name     General Compatibility     Superseded Templater	CiscoRA Prop Request Handing Edensions	ates (LAB-D erties Issuance Requin Oystography Security	C-RTP.micham     Rever
Certification Authority (Local)     Certificate Templates (LAB-DC-RTP.micham     With Internet Information Services (IIS) Manager	CA Exchang Key Recover Domain Cor Workstation RAS and IAS Kerberos Au CiscoRA User	To modify an extension, Extensions included in th Application Policies Basic Constraints Cestificate Template Issuance Policies Key Usage	select it, and then o	lick Edt.	
	User Signati Smartcard U Authenticat Smartcard L Basic EFS Administrat EFS Recover	Description of Applicatio	n Policies:		Edt

- 표시되는 창에 표시된 정책을 모두 제거합니다.
- Subject Name(주체 이름) 탭을 선택하고 Supply in Request(요청에서 공급) 라디오 버튼을 선택합니다
- 보안 탭을 선택하고 표시된 모든 그룹/사용자 이름에 대한 모든 권한을 부여합니다

CiscoRA Prop	erties	? X
General Compatibility Request Handling Subject Name	Cryptography Ke Issuance Requireme	y Attestation nts
Superseded Templates Extensions	Security	Server
Group or user names:		
Administrator Administrator Domain Admins (MICHAMEN1\Domain Enterprise Admins (MICHAMEN1\Enter	Admins) prise Admins)	
Permissions for Authenticated Users	Add R	emove Deny
Full Control	⊻	
Read	⊻	
Write	⊻	
Enrol	⊻	
Autoenroll For special permissions or advanced setting Advanced.	s, click Adv	anced
OK Cancel	Apply	Help

### 인증서 템플릿을 발급할 수 있도록 설정

- MMC 스냅인에서 Certification Authority(인증 기관)를 선택하고 폴더 트리를 확장하여 Certificate Templates(인증서 템플릿) 폴더를 찾습니다
- Name(이름) 및 Intended Purpose(목적)가 포함된 프레임의 공백을 마우스 오른쪽 단추로 클 릭합니다.
- 발급할 새 및 인증서 템플릿 선택
- 새로 만들고 편집한 CiscoRA 템플릿을 선택합니다



Active Directory CiscoRA 계정 생성

- MMC 스냅인으로 이동하여 Active Directory 사용자 및 컴퓨터를 선택합니다
- 맨 왼쪽 창의 트리에서 Users 폴더를 선택합니다
- 이름, 유형 및 설명이 포함된 프레임의 공백을 마우스 오른쪽 단추로 클릭합니다
- 새 및 사용자 선택
- 사용자 이름/비밀번호로 CiscoRA 계정(이 실습에 대해 ciscora/Cisco123이 사용됨)을 생성하 고 표시된 경우 Password never expires(비밀번호가 만료되지 않음) 확인란을 선택합니다



### IIS 인증 및 SSL 바인딩 컨피그레이션

사용 NTLM 인증

- MMC 스냅인으로 이동하고 IIS(인터넷 정보 서비스) 관리자 스냅인 아래에서 서버 이름을 선 택합니다
- 기능 목록이 다음 프레임에 표시됩니다. 인증 기능 아이콘 을 두 번 클릭합니다



 Windows Authentication을 강조 표시하고 Actions(작업) 프레임(오른쪽 창)에서 Enable(활성 화) 옵션을 선택합니다



• Actions(작업) 창에 Advanced Settings(고급 설정) 옵션이 표시됩니다. 이 옵션을 선택하고 Enable Kernel-mode authentication(커널 모드 인증 활성화)의 선택을 취소합니다

CO I HAB-OC-RTP				<b>₩</b> = \$ 0
Connections Q, • 🔜   🖄   🔕, _ 🔩 Start Page	Authentication Group by: No Grouping			Alerts Alerts Click here to learn how to configure Extended Protection
Application Pools     Stes	Name Anonymous Authentication ASP.NET Impersonation Windows Authentication	Status Enabled Disabled Enabled	Response Type HTTP 401 Challenge	Actions Disable Advanced Settings Providers
	Ad Extended Protection: Off v Click here for more information onl Enable Kernel-mode authentical By default, IS enables kernel-mode authentication performance and p	ins ins e authentication, w revent authenticati	s ? X	₽ Help

• Providers(사업자)를 선택하고 NTML을 선택한 다음 Negotiate(협상)를 순서대로 지정합니다.

Connections B,• 🔜   🖄   🚱,	Authentication			Alerts
Start Page	Group by: No Grouping .			Configure Extended Protection
Application Pools p - R Sites	Name Anonymous Authentication ASP NET Impersonation Windows Authentication	Status Enabled Disabled Enabled	Response Type HTTP 401 Challenge	Actions Disable Advanced Settings
	Enabled Providers: NELM Negotiate Negotiate/Kerberos	Providers	Nove Up Move Down	Providers
	Select a provider from the list to add it to the enabled provid Available Providers:	of available provide ers.	rs and click Add	

#### 웹 서버에 대한 ID 인증서 생성

그렇지 않은 경우, 웹 서버의 인증서가 자체 서명된 경우 CiscoRA에서 연결할 수 없기 때문에 CA에 서 서명한 웹 서비스에 대한 인증서 및 ID 인증서를 생성해야 합니다.

• IIS 스냅인에서 웹 서버를 선택하고 서버 인증서 기능 아이콘을 두 번 클릭합니다.



 기본적으로 여기에 나열된 인증서 하나가 표시됩니다. 이는 자체 서명 루트 CA 인증서입니다. Actions(작업) 메뉴에서 Create Domain Certificate(도메인 인증서 생성) 옵션을 선택합니다. 새 인증서를 만들기 위해 구성 마법사에 값을 입력 합니다. 일반 이름이 확인 가능한 FQDN(Fully Qualified Domain Name)인지 확인한 후 다음을 선택합니다.

C C I + LALOCATE +					10 H S 10 +
Connections	Server Cert	ificates			Actions Import
A LAB-CC-RTP (MOHIMENTIA	Use this feature to request	t and manage certificates that the W	eb server can use with websites config	parent Poir SSL.	Create Cettificate Report
Application Peols	Filter.	<ul> <li>Y So - Show M   Great</li> </ul>	Phyl. No Grouping •		Contraction Contraction
a 😜 Default Web Site	Name *	LAB-DC-RTP	LAB-DC-RTP	Exploration Date 2/26/2024 4:34:42	Create Self-Signed Cettificate.
s 🖓 CetSv		Create Certif	icate	7 ×	Enable Automatic Rabind of Renewed Certificate
	Specify the required information name	Name Properties aton for the cettificate. State/provin not contain abbreviations. [L&B-CC-IIS-michamen.com	a and City/locality must be specified	-	
	Organization Organizational unit: City/locality	Caco TAC RTP	1		
	State/province Country/region	MC VS	j•	E	

• 발급자가 될 루트 CA의 인증서를 선택하고 Finish(마침)를 선택합니다.

Create Certificate	?	x
Online Certification Authority		
Specify the certification authority within your domain that will sign the certificate. A friendly name is require and should be easy to remember.  Specify Online Certification Authority:  LAB-DC-RTP\LAB-DC-RTP.michamen.com Example: CertificateAuthorityName\ServerName Friendly name:  Web Cert issued by LAB-DC-RTP	red	
Previous Next Finish	Cance	

• CA 인증서 및 웹 서버의 ID 인증서가 모두 표시됩니다.



웹 서버 SSL 바인딩

 트리 보기에서 사이트를 선택하고(기본 웹 사이트를 사용하거나 특정 사이트로 좀 더 세분화 할 수 있음) 작업 창에서 바인딩을 선택합니다. 웹 사이트에 대한 바인딩을 생성, 편집 및 삭제 할 수 있는 바인딩 편집기가 나타납니다. 사이트에 새 SSL 바인딩을 추가하려면 Add를 선택 합니다.



• 새 바인딩의 기본 설정은 포트 80에서 HTTP로 설정됩니다. Type 드롭다운 목록에서 https를 선택합니다. SSL Certificate 드롭다운 목록에서 이전 섹션에서 생성한 자체 서명 인증서를 선 택한 다음 OK를 선택합니다.

			Site	Bindings	? >
Type http	Host Name	Port 80	IP Address	Binding Informa	Add Edit
			Add Site Bi	nding	2 X emove
	pe: tps v ist name: Require Server Nar	All Unass	igned n	443	
	and the star				

• 이제 사이트에 새 SSL 바인딩이 있으며, 메뉴에서 Browse \*:443 (https) 옵션을 선택하여 작동 하는지 확인하고 기본 IIS 웹 페이지에서 HTTPS를 사용하는지 확인합니다.

	? ×				
Type	Host Name	Port 80	IP Address	Binding Informa	
https		443			Edit
					Bemove
					Browse
					Close



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.