Guida all'implementazione di Wireless BYOD per FlexConnect

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Topologia Registrazione dei dispositivi e provisioning dei supplicant Portale registrazione asset Portale di autoregistrazione Autenticazione e provisioning Provisioning per iOS (iPhone/iPad/iPod) Provisioning per Android Doppia registrazione SSID wireless BYOD Registrazione singola BYOD wireless SSID Configurazione funzionalità Configurazione della WLAN Configurazione punto di accesso FlexConnect Configurazione di ISE Esperienza utente - Provisioning iOS SSID doppio SSID singolo Esperienza utente - Provisioning di Android SSID doppio Portale I miei dispositivi **Riferimento - Certificati** Informazioni correlate

Introduzione

I dispositivi mobili stanno diventando sempre più potenti dal punto di vista computazionale e popolari tra i consumatori. Milioni di questi dispositivi sono venduti ai consumatori con Wi-Fi ad alta velocità in modo che gli utenti possano comunicare e collaborare. I consumatori sono ormai abituati all'aumento della produttività che questi dispositivi mobili portano nelle loro vite e stanno cercando di portare la loro esperienza personale nello spazio di lavoro. In questo modo si creano le esigenze di funzionalità di una soluzione BYOD (Bring Your Own Device) sul posto di lavoro.

Questo documento fornisce la distribuzione di filiali per la soluzione BYOD. Un dipendente si

connette a un SSID (Service Set Identifier) aziendale con il suo nuovo iPad e viene reindirizzato a un portale di registrazione automatica. Cisco Identity Services Engine (ISE) autentica l'utente in Active Directory (AD) aziendale e scarica un certificato con un indirizzo MAC iPad incorporato e un nome utente nell'iPad, insieme a un profilo richiedente che impone l'uso di EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) come metodo per la connettività dot1x. In base alla policy di autorizzazione dell'ISE, l'utente può connettersi usando il dot1x e accedere alle risorse appropriate.

Le funzionalità ISE delle versioni software Cisco Wireless LAN Controller precedenti alla 7.2.110.0 non supportavano i client di switching locale associati tramite i punti di accesso (AP) FlexConnect. La versione 7.2.10.0 supporta queste funzionalità ISE per i FlexConnect AP per lo switching locale e i client autenticati centralmente. Inoltre, la release 7.2.110.0 integrata con ISE 1.1.1 fornisce (ma non si limita a) queste funzionalità della soluzione BYOD per il wireless:

- Profilatura e postura del dispositivo
- Registrazione dei dispositivi e provisioning dei supplicant
- Caricamento di dispositivi personali (provisioning di dispositivi iOS o Android)

Nota: anche se supportati, altri dispositivi, come laptop e workstation wireless PC o Mac, non sono inclusi in questa guida.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Cisco Catalyst
- Controller Cisco Wireless LAN (WLAN)
- Software Cisco WLAN Controller (WLC) versione 7.2.10.0 e successive
- AP 802.11n in modalità FlexConnect
- Software Cisco ISE release 11.1.1 e successive
- Windows 2008 AD con CA (Certification Authority)
- server DHCP
- Server DNS (Domain Name System)
- Protocollo NTP (Network Time Protocol)
- Notebook, smartphone e tablet client wireless (Apple iOS, Android, Windows e Mac)

Nota: per informazioni importanti su questa versione del software, consultare le <u>note di</u> <u>versione per Cisco Wireless LAN Controller e Lightweight Access Point</u> per la <u>versione</u> <u>7.2.10.0</u>. Accedere al sito Cisco.com per ottenere le note sulla versione più recenti prima di caricare e testare il software. Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia

Per implementare e testare correttamente le seguenti funzionalità, è necessaria una configurazione di rete minima, come mostrato nel diagramma:



Per questa simulazione, è necessaria una rete con un punto di accesso FlexConnect, un sito locale/remoto con DHCP locale, DNS, WLC e ISE. L'access point FlexConnect è collegato a un trunk per verificare la commutazione locale con più VLAN.

Registrazione dei dispositivi e provisioning dei supplicant

Ènecessario registrare un dispositivo in modo che il relativo supplicant nativo possa eseguire il provisioning per l'autenticazione dot1x. In base al criterio di autenticazione corretto, l'utente viene reindirizzato alla pagina guest e autenticato dalle credenziali del dipendente. L'utente visualizza la pagina di registrazione del dispositivo, in cui vengono richieste le informazioni sul dispositivo. Il processo di provisioning dei dispositivi viene quindi avviato. Se il sistema operativo non è supportato per il provisioning, l'utente viene reindirizzato al portale di registrazione degli asset per contrassegnare il dispositivo per l'accesso MAB (MAC Authentication Bypass). Se il sistema operativo è supportato, viene avviato il processo di registrazione e viene configurato il supplicant nativo del dispositivo per l'autenticazione dot1x.

Portale registrazione asset

Il portale di registrazione degli asset è l'elemento della piattaforma ISE che consente ai dipendenti di avviare l'onboarding degli endpoint tramite un processo di autenticazione e registrazione.

Gli amministratori possono eliminare le risorse dalla pagina Identità endpoint. Ogni dipendente è in grado di modificare, eliminare ed inserire in una lista nera le risorse registrate. Gli endpoint della lista nera vengono assegnati a un gruppo di identità della lista nera e viene creato un criterio di autorizzazione per impedire l'accesso alla rete da parte degli endpoint della lista nera.

Portale di autoregistrazione

Nel flusso CWA (Central Web Authentication) i dipendenti vengono reindirizzati a un portale che consente di immettere le credenziali, eseguire l'autenticazione e immettere le specifiche della risorsa specifica che si desidera registrare. Questo portale è denominato Portale self-provisioning ed è simile al Portale di registrazione dei dispositivi. Consente ai dipendenti di immettere l'indirizzo MAC e una descrizione significativa dell'endpoint.

Autenticazione e provisioning

Dopo aver selezionato il portale di autoregistrazione, i dipendenti devono fornire un insieme di credenziali valide per passare alla fase di attivazione. Dopo l'autenticazione, è possibile eseguire il provisioning dell'endpoint nel database degli endpoint e generare un certificato per l'endpoint. Un link nella pagina consente al dipendente di scaricare la procedura guidata del programma pilota per i supplicant (SPW).

Nota: per visualizzare la <u>matrice delle</u> funzionalità FlexConnect per BYOD, consultare l'articolo di Cisco sulla matrice delle funzionalità di FlexConnect.

Provisioning per iOS (iPhone/iPad/iPod)

Per la configurazione EAP-TLS, ISE segue il processo di registrazione OTA (Over-the-Air) di Apple:

- Una volta completata l'autenticazione, il motore di valutazione valuta i criteri di provisioning del client, generando un profilo supplicant.
- Se il profilo supplicant è per l'impostazione EAP-TLS, il processo OTA determina se l'ISE utilizza la firma automatica o la firma di una CA sconosciuta. Se una delle condizioni è vera, all'utente viene richiesto di scaricare il certificato di ISE o CA prima di poter iniziare il processo di registrazione.
- Per altri metodi EAP, ISE spinge il profilo finale dopo la corretta autenticazione.

Provisioning per Android

Per motivi di sicurezza, l'agente Android deve essere scaricato dal sito Marketplace Android e non può essere eseguito il provisioning da ISE. Cisco carica una versione finale della procedura guidata nel marketplace Android tramite l'account Cisco Android Marketplace Publisher.

Questo è il processo di provisioning Android:

- 1. Cisco utilizza il Software Development Kit (SDK) per creare il pacchetto Android con estensione .apk.
- 2. Cisco carica un pacchetto nel marketplace Android.
- 3. L'utente configura il criterio nel provisioning del client con i parametri appropriati.
- 4. Dopo la registrazione del dispositivo, l'utente finale viene reindirizzato al servizio di provisioning client quando l'autenticazione dot1x non riesce.
- 5. La pagina del portale di provisioning fornisce un pulsante che reindirizza gli utenti al portale del marketplace Android, dove possono scaricare l'SPW.
- 6. Viene avviato Cisco SPW che esegue il provisioning del richiedente: SPW rileva l'ISE e scarica il profilo da ISE.SPW crea una coppia certificato/chiave per EAP-TLS.SPW effettua una chiamata di richiesta proxy SCEP (Simple Certificate Enrollment Protocol) ad ISE e ottiene il certificato.I profili wireless vengono applicati da SPW.Se i profili vengono applicati correttamente, SPW attiva la riautenticazione.L'SPW si chiude.

Doppia registrazione SSID wireless BYOD

Questo è il processo per la registrazione automatica della doppia SSID wireless BYOD:

- 1. L'utente viene associato all'SSID guest.
- 2. L'utente apre un browser e viene reindirizzato al portale per gli ospiti di ISE CWA.
- 3. L'utente immette il nome utente e la password di un dipendente nel portale guest.
- 4. ISE autentica l'utente e, in base al fatto che si tratta di un dipendente e non di un ospite, reindirizza l'utente alla pagina guest di registrazione del dispositivo dipendente.
- 5. L'indirizzo MAC è precompilato nella pagina guest di registrazione del dispositivo per DeviceID. L'utente immette una descrizione e accetta la politica d'uso accettabile (AUP, Acceptable Use Policy) se necessario.
- 6. L'utente seleziona Accetta e inizia a scaricare e installare l'SPW.
- 7. Il provisioning del richiedente per il dispositivo dell'utente viene eseguito insieme a tutti i certificati.
- 8. Si verifica il CoA e il dispositivo si riassocia all'SSID aziendale (CORP) e si autentica con EAP-TLS (o altro metodo di autorizzazione in uso per il richiedente).

Registrazione singola BYOD wireless SSID

In questo scenario, esiste un singolo SSID per l'accesso aziendale (CORP) che supporta sia PEAP (Protected Extensible Authentication Protocol) che EAP-TLS. Nessun SSID guest.

Questo è il processo per la registrazione automatica della BYOD wireless con un solo SSID:

- 1. L'utente viene associato a CORP.
- 2. L'utente immette un nome utente e una password dipendente nel supplicant per l'autenticazione PEAP.
- 3. ISE autentica l'utente e, in base al metodo PEAP, fornisce una policy di autorizzazione di accettazione con reindirizzamento alla pagina guest di registrazione del dispositivo dipendente.

- 4. L'utente apre un browser e viene reindirizzato alla pagina guest di Registrazione dispositivo dipendente.
- 5. L'indirizzo MAC è precompilato nella pagina guest di registrazione del dispositivo per DeviceID. L'utente immette una descrizione e accetta le CDS.
- 6. L'utente seleziona Accetta e inizia a scaricare e installare l'SPW.
- 7. Il provisioning del richiedente per il dispositivo dell'utente viene eseguito insieme a tutti i certificati.
- 8. Si verifica il CoA e il dispositivo si riassocia all'SSID CORP e si autentica con EAP-TLS.

Configurazione funzionalità

Per iniziare la configurazione, completare i seguenti passaggi:

1. Per questa guida, verificare che la versione del WLC sia 7.2.10.0 o successiva.

ululu cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Monitor	Summary					
Summary Access Points Cisco CleanAir Statistics CDP Rogues	-ili-ili- cisco	ess Points Supporte		Cisco 250	O Series Wireless O	Controller Model 2504
Clients	Controller Summ	ary		Ro	gue Summary	
Multicast	Management IP Address	10.10.10.5		A	tive Rogue APs	
	Software Version	7.2.104.16		A	tive Rogue Clients	
	Field Recovery Image Version	1.0.0		A	thoc Rogues	
	System Name	wic-11mor		R	ogues on Wined Net	WORK

2. Passare a Sicurezza > RADIUS > Autenticazione e aggiungere il server RADIUS al WLC.

uluili. cisco	MONITOR	WLANS (CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDB	ACK
Security	RADIUS	Authentica	ation Serve	rs					
AAA General RADIUS Authentication Accounting Fallback	Call Stat Use AES MAC De	tion ID Type ¹ Key Wrap limiter	System Mi	AC Address 1 for FIPS custome	ers and requir	es a key wrap com	pliant RADIUS se	rver)	
TACACS+ LDAP	Network User	Managemen	Server t Index	Server Addre	ss Port		Sec	Admin Status	
MAC Filtering Disabled Clients User Login Policies	2	2	1	10.10.10.60	1812	D	sabled	Enabled	

3. Aggiungere ISE 1.1.1 al WLC:

Immettere un segreto condiviso.Impostare il supporto per RFC 3576 su Enabled.

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
RADIUS Authent	ication Server	s > Edit					
Server Index		1					
Server Address		10.10.10.60					
Shared Secret Form	at	ASCII :					
Shared Secret							
Confirm Shared Sec	ret						
Key Wrap	0	(Designed fo	r FIPS custom	ers and requires a l	key wrap complia	nt RADIU	S server)
Port Number		1812					
Server Status		Enabled :					
Support for RFC 357	76	Enabled :					
Server Timeout		2 second	ds				
Network User		Enable					
Management		Enable					
IPSec		Enable					

4. Aggiungere lo stesso server ISE come server di accounting RADIUS.

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANA
RADIUS Account	ing Servers >	Edit		
Server Index	1			
Server Address	10.1	0.10.60		
Shared Secret Forma	t ASC	1I +		
Shared Secret				
Confirm Shared Secret	et			
Port Number	1813			
Server Status	Enal	bled :		
Server Timeout	2	seconds		
Network User	🗹 E	nable		
IPSec		Enable		

 Creare un ACL WLC Pre-Auth da usare nella policy ISE in un secondo momento. Selezionare WLC > Security > Access Control Lists > ACL FlexConnect, quindi creare un nuovo ACL FlexConnect denominato ACL-REDIRECT (nell'esempio).

cisco		<u>W</u> LANs		WIR
Security	FlexConr	nect Ac	cess Control L	ists
 AAA Local EAP Priority Order Certificate Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs	Acl Name	ECT		
Wireless Protection				

6. Nelle regole ACL, autorizzare tutto il traffico da/verso l'ISE e autorizzare il traffico dei client durante il provisioning del supplicant.

Per la prima regola (sequenza 1):

Impostare Source (Origine) su **Any (Qualsiasi)**.Impostare IP (indirizzo ISE)/ Netmask **255.255.255.1**mpostare Action su **Permit**.

Access Control List	ts > Rules > Edit		
Sequence	1		
Source	Any :		
		IP Address	Netmask
Destination	IP Address ‡	10.10.10.60	255.255.255.255
Protocol	Any		
DSCP	Any ÷		
Direction	Any :		
Action	Permit ‡		

Per la seconda regola (sequenza 2), impostare source IP (indirizzo ISE)/ mask 255.255.255.255 su **Any** and Action to **Permit**.

Gene	ral									
Access	s List Name	ACL-RED	IR	ECT						
Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCI	,
1	Permit	0.0.0.0 0.0.0.0	/	10.10.10.60 255.255.255.255	/	Any	Any	Any	Any	
2	Permit	10.10.10.60 255.255.255.255	/	0.0.0.0	/	Any	Any	Any	Any	

7. Creare un nuovo gruppo FlexConnect denominato Flex1 (in questo esempio):

Passare alla scheda **Gruppo FlexConnect > Criteri Web**.Nel campo ACL WebPolicy, fare clic su **Add**, quindi selezionare **ACL-REDIRECT** o l'ACL FlexConnect creato in precedenza.Confermare che popola il campo **Elenchi di controllo di accesso di WebPolicy**.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBA	Sage Configuration Bing Logout Befi NCK
Wireless	FlexConnect Groups > Edit 'Flex1'	< Back Apply
Access Points All APs Redos Bo2.11a/n B02.11b/ph Global Centiguration Advanced Mesh RF Profiles FlexConnect Groups PresConnect Groups B02.11a/n B02.11b/g/n	General Local Authentication Image Upgrade VLAN-ACL mapping WebPolicies webPolicy Act. Act.=REDIRECT	WebPelicies

8. Fare clic su Apply and Save Configuration (Applica e salva configurazione).

Configurazione della WLAN

Per configurare la WLAN, effettuare i seguenti passaggi:

1. Creare un SSID WLAN aperto per l'esempio di SSID doppio:

Immettere il nome di una WLAN: **DemoCWA** (nell'esempio).Selezionare l'opzione **Abilitato** per Stato.

WLANs > E	dit 'Demo	CWA'	
General	Security	QoS	Advanced
Profile Na	ime	DemoC	WA
Туре		WLAN	
SSID		DemoC	WA
Status		F Enat	bled
Security I	Policies	MAC F (Modifica	iltering tions done under se
Radio Pol	icy	All	*
Interface Group(G)	/Interface	manag	ement 💌
Multicast	Vlan Feature	Enab	led
Broadcas	t SSID	₩ Enab	led

2. Passare alla scheda Sicurezza > scheda Layer 2 e impostare i seguenti attributi:

Sicurezza di livello 2: **nessuna**Filtro MAC: **Abilitato** (casella selezionata)Transizione rapida: **disabilitata** (casella non selezionata)

LANs > E	dit 'Demo(CWA'	
General	Security	QoS	Advanced
Layer 2	Layer 3	AAAS	ervers
Layer 2	Security 🤨 🚺	lone	
	414	C ritterin	
Fast Tran	sition	C riiterin	<u>}−</u> (*

3. Andare alla scheda **AAA Server** e impostare i seguenti attributi:

A	uten	ticaz	zione	e server	account:	Abilitat	oServer	1: •	<ise ip<="" th=""><th>addre:</th><th>ss></th></ise>	addre:	ss>
_											

Layer 2 Lay	er 3 AAA Ser	vers	
Select AAA server	s below to overrid	le use of default servers on	this WLAN
Radius Servers			
Radius Servers	Overwrite interface	Enabled	
Radius Servers	Overwrite interface	Enabled	Accounting Servers
Radius Server	Overwrite interface	Enabled Authentication Servers Enabled IP:10.10.10.60, Port:1812	Accounting Servers Enabled IP:10.10.10.60, Port:181
Radius Server Server 1 Server 2	Overwrite interface	Enabled Authentication Servers Enabled IP:10.10.10.60, Port:1812 None	Accounting Servers Enabled IP:10.10.10.60, Port:181 None

4. Scorrere verso il basso dalla scheda **Server AAA**. In Ordine di priorità autenticazione per l'utente con autenticazione Web verificare che **RADIUS** sia utilizzato per l'autenticazione e che gli altri non siano utilizzati.

Authentication priorit web-auth user	y order for	-	
Not Used LOCAL LDAP	>	Order Used For Authentication	Up Down

5. Andare alla scheda Advanced (Avanzate) e impostare i seguenti attributi:

Allow AAA Override	₩ Enabled	2002.7
Coverage Hole Detection	P Enabled	DeCP Server Coverna
Enable Section Timeout	gr (1800 Session Timesut (sess)	CHCP Adds. Assignment C Amazine
Aironat 18	P Enabled	Nanapagement Frame Protection (NFP
Diagnostic Channel	L'Evabled	
Override Interface ACL	IPut None R IPut None R	MPP Class Protection . Optional
F2F Blocking Action	Disabled (#	BTD9 Period (in beacan intervals)
Clant Exclusion	["Evabled	
Maximum Allowed Clients	F	802.33.wh (3 - 298) [3 802.333/g/n (3 - 299) [3
Static IF Tunneling 🛤	L'Enabled	NAC
Wi-Fi Direct Clients Policy	Disabled R	NAC State Radius NAC .
Recimum Allowed Clarify Far AF Radio	[298	Cleart Load Balancing and Balancing

Consenti sostituzione AAA: abilitataStato NAC: Radius NAC

Nota: RADIUS Network Admission Control (NAC) non è supportato quando FlexConnect AP è in modalità disconnessa. Pertanto, se l'access point FlexConnect è in modalità standalone e perde la connessione al WLC, tutti i client vengono disconnessi e l'SSID non viene più annunciato.

6. Scorrere verso il basso nella scheda Advanced e impostare FlexConnect Local Switching su **Enabled**.



7. Fare clic su Apply and Save Configuration (Applica e salva configurazione).



8. Creare un SSID WLAN 802.1X denominato **Demo1x** (nell'esempio) per gli scenari a SSID singolo e doppio.

WLANs > Edit 'Demo	1x'
General Security	QoS Advanced
Profile Name	Demoix
Туре	WLAN
SSID	Demo1x
Status	Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under secu
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	Enabled

9. Passare alla scheda Sicurezza > scheda Layer 2 e impostare i seguenti attributi:

Sicurezza di layer 2: **WPA+WPA2**Transizione rapida: **disabilitata** (casella non selezionata)Gestione chiavi di autenticazione: 802.IX: **Abilita**

LANs > E	dit 'Demo	1x'		
General	Security	QoS	Advar	nced
Layer 2	Layer 3	AAA S	ervers	
Laver 2	Security 1	WPA+WPA	2	-
cayer z	M	AC Filterin	° 02 □	-
Fast Trans	ition			
Reassociation	s I on Timeout 20 2 Parameter	rs		
WPA Pol	licy			
WPA2 P	olicy	₹		
WPA2 E	ncryption	I⊽ AE	s E	TKIP
Authentica	ation Key Ma	nagemen	t	
802.1X	₹ E	inable	_	
CCKM	Π ε	nable		
neu	E .			

10. Andare alla scheda Advanced (Avanzate) e impostare i seguenti attributi:

Consenti sostituzione AAA: abilitataStato NAC: Radius NAC

Now AAA Override	P Enabled	0407
Coverage Hole Detection	W Enabled	DHCP Server Coverride
Inable Session Timesult	gr [1800	
inunat II	Second Trimeout (seco)	Dece and assignment [Assaired
Samuels Channel	Crushe	Nanagement Frame Protection (NFP)
Iverride Interface ACL	Put Store B Put Store B	MR Class Budgetters . Cottoned
OF Blocking Action	[Disabled]	BTIN Period (in beauty interaction)
Sant Exclusion	Rended 60	And the second second second second
	Timeout Value (secs)	802.33 m/s (3 - 299) 5
Santa #	9	802.13b/g/h (1 - 255) 1
	France	NAC
Madels 100 Wassenakings 20	1 Strategiese Strategie	

11. Scorrere verso il basso la scheda **Advanced** (Avanzate) e impostare FlexConnect Local Switching su **Enabled** (Abilitato).

Enabled
· P susses

12. Fare clic su **Apply** and **Save Configuration** (Applica e salva configurazione).



13. Confermare che entrambe le nuove WLAN sono state create.

MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs								Entries 1 - 5 of !
Current Fil	ter: Nor	ne [Change	Filter] [Clear	Filter]	1	Create New	• 6	0
U WLAN J	D Туре	Profile Na	me	v	VLAN SSID		Admin Status	Security Policies
E 1	WLAS	85×			LEH .		Disable	[[#PAJ][Av84(802.1X]]
C 2	WLAN						Enabled	[#PA2][Auth(PS2)]
□ <u>2</u>	WLAN	Demo1x		C	Demo1x		Enabled	[WPA2][Auth(802.1X)]
	WLAN	DemoCWA		C	DemoCWA		Enabled	MAC Filtering
Π1	91,45	fig-r			ler:		Creative	I Web-Auth

Configurazione punto di accesso FlexConnect

Per configurare l'access point FlexConnect, completare i seguenti passaggi:

1. Passare a WLC > Wireless e fare clic sull'access point FlexConnect di destinazione.

MONITOR	<u>W</u> LANs		WIRELESS
All APs			
Current Fil	ter		None
Number o	f APs		2
AP Name		AP	Model
Site-B-Flex		AI	R-LAP1262N-A-K

2. Fare clic sulla scheda FlexConnect.



3. Abilitare il supporto VLAN (la casella è selezionata), impostare l'ID VLAN nativo e fare clic su **Mapping VLAN**.

VLAN Support	2	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Cont	figured 😡

4. Impostare l'ID VLAN su 21 (in questo esempio) per l'SSID per la commutazione locale.

ONITOR	t <u>W</u> LANs	CONTROLLER	WIRELESS	SECURI
II APs	> Site-B-	-FlexAP > VLA	N Mapping	s
AP Nam	•	Site-B-FleyAP		
Base Ra	dio MAC	e8:04:62:0a:68:80	0	
WLAN (d	SSID			VLAN ID
3	Demo1x			21
4	DemoCW	A		21
				8
	-			and the second sec

5. Fare clic su Apply and Save Configuration (Applica e salva configurazione).

Configurazione di ISE

Per configurare l'ISE, completare la procedura seguente:

1. Accedere al server ISE: <https://ise>.

	Identity Services Engine Uservarie admin Passeori Banenber uservarie Poblen logging in ³
effliates in the US and certain other countries.	cisco

2. Passare a Amministrazione > Gestione identità > Origini identità esterne.



3. Fare clic su Active Directory.



4. Nella scheda Connessione:

Aggiungere il nome di dominio di **corp.rf-demo.com** (in questo esempio) e impostare il nome predefinito dell'archivio identità su **AD1**.Fare clic su **Salva configurazione**.Fare clic su **Partecipa** e specificare il nome utente e la password dell'account dell'amministratore di Active Directory necessari per l'aggiunta.Lo stato deve essere verde. Abilita **Connesso a:** (casella selezionata).

Connection Advance	ced Settings	Groups	Attributes	
	* D	omain Name co	p.rf-demo.com	
	* Identity	Store Name AD	1	
One or more nodes may be s Connection.	selected for Join	n or Leave operat	ions. If a node is joined	then a leave operation is r
One or more nodes may be s Connection.	selected for Joir	n or Leave operat	ions. If a node is joined	then a leave operation is r
One or more nodes may be s Connection. 연결 Join 연결 Leave 연결 Te	selected for Joir	n or Leave operat	ions. If a node is joined Status	then a leave operation is r

5. Eseguire un test di connessione di base ad Active Directory con un utente del dominio corrente.

oonneedon.	
👷 Join 🛛 👷 Leave	👷 Test Connection 👻
ISE Node	Basic Test
✓ ise11-mnr	Detailed Test
Test Connection * User Name: paul * Password:	×

6. Se la connessione ad Active Directory ha esito positivo, una finestra di dialogo conferma che la password è corretta.



7. Passare a Amministrazione > Gestione identità > Origini identità esterne:

Fare clic su **Profilo di autenticazione certificato**. Fare clic su **Add** (Aggiungi) per un nuovo profilo di autenticazione del certificato (CAP).

cisco Identity Services	Engine		
🛕 Home Operations 🔻	Policy 🔻 Administratio	on 🔻	
🔆 System 🥻 👰 Identity Ma	anagement 📰 Netwo	ork Resources 🛛 🛃 Web P	ortal Manage
Identities Groups Extern	al Identity Sources Ide	entity Source Sequences S	iettings
External Identity Sources	C	ertificate Authenticatio	n Profile
∲•	ŵ.	In July Dente	
Certificate Authentication Profil	e 📀 🗧	Earc Add 4 Dupic	ate 🗡 De
Active Directory	L	Name 🐱	
CDAP LDAP	۲		
RADIUS Token	۲		
RSA SecurID			

8. Immettere il nome **CertAuth** (in questo esempio) per il criterio di autorizzazione delle connessioni; per l'attributo Nome utente principale X509, selezionare **Nome comune**, quindi fare clic su **Invia**.

* Name	CertAuth	
Description		
Principal Username X509 Attribute	Common Name	¥
Perform Binary Certificate Comp	arison with Certificate retrieved	from LDAP or Active Directory
DAP/AD Instance Name		

9. Confermare l'aggiunta del nuovo criterio di autorizzazione delle connessioni.

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admini	stration 🔻
🔆 System 🦉 Identity Management 📰	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
♦•	
Certificate Authentication Profile	
Active Directory	U Name
🛅 LDAP 💿	Cerbasin
RADIUS Token 3	
RSA SecurID 🛞	

10. Passare a Amministrazione > Gestione identità > Sequenze origine identità e fare clic su Aggiungi.

cisco Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Ad	ministration 🔻
🔆 System 🛛 👰 Identity Management	Network Resources 🛃 Web Portal Management
Identities Groups External Identity Source	es Identity Source Sequences Settings
Identity Source Sequence	
Name S	Description
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Po
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal

11. Assegnare alla sequenza il nome **TestSequence** (nell'esempio).

cisco Id	entity Services Engine
💧 Home	Operations Policy Administration
🔆 System	Veb Portal Mana
Identities (Groups External Identity Sources Identity Source Sequences Settings
Identity Source Sequence Identity Source Sequence Identity Source Sequence	rce Sequence
* Name	TestSequence
Description	
 Certificate 	Based Authentication

12. Scorrere fino a Autenticazione basata su certificato:

Abilitare **Seleziona profilo di autenticazione certificato** (la casella è selezionata).Selezionare **CertAuth** (o un altro profilo CAP creato in precedenza).

Certificate Based Authentication	
Select Certificate Authentication Profile	CertAuth *
 Authentication Search List 	

13. Scorri verso il basso fino all'elenco di ricerca autenticazione:

Sposta AD1 da Disponibile a Selezionato.Fare clic sul pulsante su per spostare AD1 alla priorità superiore.

 Authentication Search Lis 	t		
A set of identity sources that will be accessed in sequence until first authentication succeeds			
Available		Selected	_
	*	Internal Users Internal Endpoints	×
	*		V V

14. Per salvare, fare clic su Submit (Invia).



15. Confermare l'aggiunta della nuova sequenza di origine identità.

CISCO Identity Services Engine		
🛕 Home Operations 🔹 Policy 💌 Administrat	tion 🔻	
🔆 System 🛛 🖉 Identity Management 🖉 Netw	vork Resources 🚯 Web Portal Management	
Identities Groups External Identity Sources	Sentity Source Sequences Settings	
Identity Source Sequence		
And dette Department Marine		
Lest Arves HT protectes Y passe		
Name -	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users
TestSequence		CertAuth, Internal Users, Internal Endpoints

 Utilizzare AD per autenticare il portale dei dispositivi personali. Selezionare ISE > Amministrazione > Gestione identità > Sequenza origine identità, quindi modificare MyDevices_Portal_Sequence.

🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web
Identities Groups External Identity Source	Identity Source Sequences
dentity Source Sequence	
/ Edit 🕂 Add 🖓 Duplicate 🗙 Delete	
/Edit 🛖Add 🖓Duplicate 🗙Delete	Description
/ Edit + Add Duplicate X Delete	Description A Built-in Identity Sequence
Edit + Add Duplicate XDelete Name Guest_Portal_Sequence MyDevices_Portal_Sequence	Description A Built-in Identity Sequence A Built-in Identity Sequence
Edit + Add Duplicate XDelete Name Guest_Portal_Sequence MyDevices_Portal_Sequence Sponsor_Portal_Sequence	Description A Built-in Identity Sequence A Built-in Identity Sequence A built-in Identity Sequence

17. Aggiungere **AD1** all'elenco Selezionati e fare clic sul pulsante su per spostare AD1 alla priorità superiore.



18. Fare clic su Salva.



19. Confermare che la sequenza dell'archivio identità per MyDevices_Portal_Sequence contenga AD1.



20. Ripetere i passaggi da 16 a 19 per aggiungere AD1 per Guest_Portal_Sequence e fare clic su **Salva**.



21. Confermare che Guest_Portal_Sequence contenga AD1.

Name .	Description	Identity Stores
Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
Contraction of the second s		

22. Per aggiungere il WLC al dispositivo di accesso alla rete (WLC), selezionare Amministrazione > Risorse di rete > Dispositivi di rete, quindi fare clic su Aggiungi.

cisco Identity Services Engine	
♦ Home Operations ▼ Policy ▼ Adminis	stration 🔻
Network Devices Network Device Groups Exte	rnal RADIUS Servers RADIUS Server Sequences S
Network Devices	Network Devices
• p ••• @•	/ Edit Add Duplicate @Import
Network Devices Default Device	Name A IP/Mask Location

23. Aggiungere il nome del WLC, l'indirizzo IP, la subnet mask e così via.

Network Devices List > New Net	twork Device	
Network Devices		
 Name Description 	WLC	
* IP Address:	10.10.10.5	/ 32
Model Name Software Version		
* Network Devic	e Group	
Location	All Locations	Set To Default
Device Type	All Device Types	Set To Default

24. Scorrere fino a Impostazioni di autenticazione e immettere il segreto condiviso. Deve corrispondere al segreto condiviso del RADIUS del WLC.

	Enable Authentication Settings		
	Protocol	RADIUS	
	 Shared Secret 	•••••	Show
	Enable KeyWrap		
	 Key Encryption Key 		Show
	 Message Authenticator Code Key 		Show
	Key Input Format	ASCII HEX	ADECIMAL
SNMP Settings			
N CCA Attributer			

- 25. Fare clic su Invia.
- 26. Selezionare ISE > Policy > Policy Elements > Results (Risultati criteri).

CISCO Identity Service	es Engine
🛕 Home Operations 🔻	Policy Administration
System A Identity I Network Devices Network I Network Devices	 Authentication Authorization Profiling Posture Client Provisioning Security Group Access
Network Devices	Egress Policy Network Device Authorization
E Default Device	Policy Elements Dictionaries Conditions Results

27. Espandere **Risultati** e **autorizzazione**, fare clic su **Profili di autorizzazione**, quindi fare clic su **Aggiungi** per un nuovo profilo.

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admin	istration 🔻
🛃 Authentication 💿 Authorization 🔀 F	Profiling 🕜 Posture 😡 Client Provisioning
Dictionaries Conditions Results	
Results	Standard Authorization Profiles
(<u></u>	/ Edit Add Duplicate X Delete
Authentication	Name Name Blacklist Access
* 🧱 Authorization	Gron IP Phones
Authorization Profiles	ContractV12
Garage Blacklist_Access	DenvAccess

28. Assegna al profilo i seguenti valori:

Nome: CWA

Authorization Profiles > Authorization I	New Authorization Profile Profile
* Name	CWA
Description	
* Access Type	ACCESS_ACCEPT

Abilita autenticazione Web (casella selezionata):

Autenticazione Web: **centralizzata**ACL: **ACL-REDIRECT** (deve corrispondere al nome dell'ACL di preautenticazione WLC).Reindirizzamento: **predefinito**

▼ Common Tasks							
DACL Name							
Voice Domain Permissio	n						
Web Authentication	Centralized	*	ACL	ACL-REDIRECT	Redirect	Default	٣

29. Fare clic su Invia e verificare che il profilo di autorizzazione CWA sia stato aggiunto.



30. Per creare un nuovo profilo di autorizzazione, fare clic su Add (Aggiungi).



31. Assegna al profilo i seguenti valori:

Nome: Provisioning

Authorization Profiles > Authorization I	New Authorization Profile Profile
* Name	Provision
Description	
* Access Type	ACCESS_ACCEPT 👻

Abilita autenticazione Web (casella selezionata):

Valore autenticazione Web: provisioning supplicant



ACL: ACL-REDIRECT (deve corrispondere al nome dell'ACL di preautenticazione WLC).

 Common Tasks 		
DACL Name		
ULAN VLAN		
Voice Domain Permission		
G Web Authentication	Supplicant Provisioning	ACL ACL-REDIRECT
Auto Smart Bort		

32. Fare clic su **Invia** e confermare che il profilo di autorizzazione del provisioning è stato aggiunto.



33. Scorrere verso il basso in Risultati, espandere Provisioning client e fare clic su Risorse.



34. Selezionare Profilo supplicant nativo.



35. Assegnare al profilo il nome WirelessSP (in questo esempio).

tive Supplicant Profi	le
* Name	WirelessSP
Description	

36. Immettere i seguenti valori:

Tipo di connessione: **wireless**SSID: **Demo1x** (questo valore deriva dalla configurazione WLC 802.1x WLAN)Protocollo consentito: **TLS**Dimensioni della chiave: **1024**

Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demoix
		Security	WPA2 Enterprise +
* Allowed Protocol	PEAP		v
Optional Settings	TLS PEAP	ę	3
Submit Cancel			

- 37. Fare clic su Invia.
- 38. Fare clic su Salva.

* Allowed Protocol	TLS	
* Key Size	1024	•
Save Reset		

39. Confermare che il nuovo profilo è stato aggiunto.

Resources				
/ Edit 🚽 Add 👻 🕒 Duplicate	XDelete			
Name	Туре			
Wireless	NativeSPProfile			

40. Passare a **Policy > Client Provisioning**.



41. Immettere i seguenti valori per la regola di provisioning dei dispositivi iOS:

Nome regola: iOSGruppi di identità: qualsiasi

	Rule Name	Identity Groups	Operating Systems	Other Conditions		
· 🖌	IOS	If Any 🛟 and	Choose a 🗢	and Condition(s)		
			Choose an Open	rating System 👷 🕂		

Sistemi operativi: Mac iOS All

Operating System Grou	ips
	P)
◆- ■ '≣	ŵ.
Android	
Mac OSX	
Mac IOS All	
🚞 Windows All	۲

Risultati: WirelessSP (profilo supplicant nativo creato in precedenza)

ther Conditions	Results
	then Result 🕀 🧙

Passare a Risultati > Profilo procedura guidata (elenco a discesa) > WirelessSP.



WizardProfile	
	Q
◆ •	- ∰-
Clear Selection	
Wireless	

42. Confermare che il profilo di provisioning iOS è stato aggiunto.

			Rule Name	I	(dentity Gr	oups		Operating Systems			Other Conditions		Results	
1	¥.	٠	105	If [Any	\diamond	and	Mac IOS All	Þ	and	Condition(s)	\$ then	WrelessSP	\diamond

43. Sul lato destro della prima regola, individuare l'elenco a discesa Azioni e selezionare **Duplica sotto** o sopra.



44. Modificare il nome della nuova regola in Android.



45. Cambiare i sistemi operativi in Android.

Operating System Gro	oups
4 = = =	(م
P*	<i>≌</i> +
 Max 1000 Max 1000 	
Windows Al	()

- 46. Non modificare altri valori.
- 47. Fare clic su Save (schermata in basso a sinistra).



48. Selezionare ISE > Policy > Authentication (Autenticazione).



49. Modificare la condizione in modo da includere Wireless_MAB ed espandere Wired_MAB.



50. Fare clic sull'elenco a discesa Nome condizione.



51. Selezionare **Dizionari > Condizione composta**.



52. Selezionare Wireless_MAB.



53. A destra della regola, selezionare la freccia da espandere.

If	Wireless_MAB	¢	allow protocols	Allowed Protocol : Default Netw	and	Ę

54. Selezionare i valori seguenti dall'elenco a discesa:

Origine identità: **TestSequence** (valore creato in precedenza)Se l'autenticazione non è riuscita: **Rifiuta**Se l'utente non è stato trovato: **Continua**Se il processo non è riuscito: **Elimina**

TestSequence 🗢
Identity Source TestSequence
Options
If authentication failed Reject
If user not found Continue
If process failed Drop 🔹

55. Passare alla regola **Dot1X** e modificare i valori seguenti:



Compound Condition
٩
🔶 🔳 🗐 🍕
Wired_MAB
Wireless_MAB
Wired_802.1X
Wireless_802.1X cha
Switch_Local_Web_Authentication
WLC_Web_Authentication
: If Wired_802.1X allo : all Add All Conditions Below t Condition Name Wireless_802.1X O

Condizione: Wireless_802.1X

Origine identità: TestSequence

Identity Source TestSequence	se for authe
Options	Identity Source List
If authentication failed Reject	
If user not found Reject	
If process failed Drop 🔹	∲•
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS	Internal Endpoints
it is not possible to continue processing when authentication fails	Internal Users
If continue option is selected in these cases, requests will be reject	Guest_Portal_Sequence
	Sponsor_Portal_Sequence
	MyDevices_Portal_Sequence
	TestSequence
Internal Users 🗢	🗉 CertAuth
	DenyAccess

56. Fare clic su **Salva**.



57. Selezionare ISE > Policy > Authorization (Policy > Autorizzazione).



58. Le regole predefinite (ad esempio Black List Default, Profiled e Default) sono già configurate dall'installazione; le prime due possono essere ignorate; la regola predefinita verrà modificata in seguito.

rst Ma	itched R	ule Applies +			
Exce	ptions (0)			
Stan	dard				
	Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
1		Black List Default	if Blacklist	then	Blacklist_Access

59. A destra della seconda regola (Telefoni IP Cisco con profilo), fare clic sulla freccia in giù accanto a Modifica e selezionare **Inserisci nuova regola sotto**.



Viene aggiunto un nuovo numero di regola standard.

	Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
1		Black List Default	f Blacklist	then Blackist_Access
		Profiled Cisco IP Phones	Cisco-IP-Phone	then Osco_IP_Phones
11	- 🖬	Standard Rule 1	f Any O and Condition(s)	then AuthZ Profil
		Default	If no matches, then PermitAccess	

60. Modificare il nome della regola da Standard Rule # a **OpenCWA**. Questa regola avvia il processo di registrazione sulla WLAN aperta (SSID doppio) per gli utenti che vengono alla rete guest per eseguire il provisioning dei dispositivi.



61. Fare clic sul segno più (+) per Condizione/i, quindi fare clic su Seleziona condizione esistente dalla libreria.

Cisco-IP-Phone		then Cisco_IP_Phone
f Any 💠 and	Select Condition	then AuthZ Pro
r no matches, then Perm	Select Existin	g Condition from Library (7) or Create

62. Selezionare Condizioni composte > Wireless_MAB.

er conditions. Drag and drop	Compound Conditions	
	(م	
	🔶 🗐 🗐 🛞 🗸	
	Wired_802.1X	
	Wired_MA8	
	Wireless_802.1X	
ups and other conditions)	Wireless_MAB	
	Catalyst_Switch_cocal_Web_Authentica	
	WLC_Web_Authentication	
	F	
Select Condition	1	
Add All Conditions B		
Condition Name		
alest and the		
Select Condition	2	

63. Nel Profilo AuthZ, fare clic sul segno più (+), quindi selezionare Standard.
| | Profiles | |
|----------------|-----------------------|--------|
| | | م
ا |
| lcy Elements | ₫- | ÷. |
| | 🚞 Inline Posture Node | ۲ |
| | Ecurity Group | ۲ |
| | Standard 🔓 | ۲ |
| rmissions | | |
| cklist_Access | | |
| co_IP_Phones | | |
| AuthZ Profil 🗢 | | |
| Select an item | 9 — ÷ | |
| | | |

64. Selezionare il CWA standard (profilo di autorizzazione creato in precedenza).



65. Confermare che la regola sia stata aggiunta con le condizioni e l'autorizzazione corrette.



66. Fare clic su Fine (sul lato destro della regola).



67. A destra della stessa regola, fare clic sulla freccia in giù accanto a Modifica e selezionare

Inserisci nuova regola sotto.



68. Modificare il nome della regola da Standard Rule # a **PEAPrule** (in questo esempio). Questa regola viene utilizzata per PEAP (utilizzato anche per uno scenario SSID singolo) per verificare che l'autenticazione di 802.1X senza Transport Layer Security (TLS) e il provisioning del supplicant di rete vengano avviati con il profilo di autorizzazione del provisioning creato in precedenza.

🖉 🗹 Open	CWA f	Wireless_MAB		then C	WA
1 🗹 - 🛛 🛛 🕅	rd Rule 1	Any 💠 and	Condition(s)	💠 the	Auth2 Profil 💠

69. Modificare la condizione in Wireless_802.1X.

ſ	Condition(s)	- then AuthZ Profil 💠	
n	Add All Conditions Below	to Library	
	Condition Name	Expression	
	Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	ŵ .

70. Fare clic sull'icona dell'ingranaggio sul lato destro della condizione e selezionare **Aggiungi attributo/valore**. Condizione 'and', non 'or'.



71. Individuare e selezionare Accesso alla rete.

		Dictionaries	
			Q
		⇔- ≡ .≡	\$\$~
os and other conditions)			<u>^</u>
	then		
	then		
	then		
Condition(s)	-		
tAccess			
Condition Name Expression	on		
Wireless_802.1X 📀 Radius:Ser	vice-Type E	Network Access	
Select A	Attribute	7	

72. Selezionare AuthenticationMethod e immettere i seguenti valori:



AuthenticationMethod: uguale a

Network Access:Au📀	•
	Equals Not Equals

Selezionare MSCHAPV2.

S Framed AND Radius:NAS-Port				
Equals 💌	v			
	CHAP/MD5			
	Lookup			
	MSCHAPV1			
	MSCHAPV2			
	PAP_ASCII			
	x509_PKI			

Questo è un esempio della regola. Accertarsi che la condizione sia AND.

and	Condition(s)	- then AuthZ Profil 💠		
	Condition Name	Expression	AND	
	Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port		ŵ•
	¢ [Network Access:Au Equals MSCHAPV2	0	ŵ.

73. In Profilo AuthZ, selezionare **Standard > Provisioning** (profilo di autorizzazione creato in precedenza).

then	AuthZ Profil		Done
	Select an item 📀	- +	

Standard	ž
	و م
⟨] = :	₩ •
Servision (h)	

74. Selezionate Fatto (Done).



75. A destra della regola PEAP, fare clic sulla freccia in giù accanto a Modifica e selezionare **Inserisci nuova regola sotto**.



76. Modificare il nome della regola da Standard Rule # a **AllowRule** (in questo esempio). Questa regola verrà utilizzata per consentire l'accesso alle periferiche registrate con certificati installati.



77. In Condizioni selezionare Condizioni composte.

A.1	Dictionaries	Asteletetetetetetetetetetetetetetetetetet
		P
	∳- ■ '≣	/@+
ant Dravisioning	Simple Conditions	۲
	Compound Conditions	R.
	Time and Date Conditions	50
Condition(s)		h
Add All Conditions B		
Condition Name		

78. Selezionare Wireless_802.1X.



79. Aggiungere un attributo AND.

Wireless_802.1X	⇔ then ♦	
Add All Conditions Belo	w to Library	
Condition Name	Expression	
Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	5

80. Fare clic sull'icona dell'ingranaggio sul lato destro della condizione e selezionare **Aggiungi attributo/valore**.



81. Individuate e selezionate Raggio (Radius).

6			Dictionaries		
	10		◆- ■ '=		
Client Provisioning 🛛 🚊 Secur	ity Group Acce	ss 🤱	Care Care		
and an			Caco-MEDM		
		these	Caco-critecture		
		then	🚞 DEHICE		
		then	🛄 EndPointer		
			🔛 Guest		
etwork Access:AuthenticationMe	thod	then	🔛 AllerityGroup		
Wireless 802.1X Network Acce	ss:A 🗢	1	🚞 Internalitier		
			Mircaell Research		
Condition Name	Expression		Betwork Access	AND	٣
			🚞 Radius	-	
Wireless_802.1X 📀	Radius:Servic	e-Type E	Season	2 <u>-</u>	
٥	Select Att	ribute 💟		o	

82. Selezionare Calling-Station-ID-[31].



83. Selezionare Uguale a.

Radius:Service-Type EQUALS	6 Framed AND Ra	dius:NAS-Port	
Radius:Calling-Statio	Founds 0		٥
	Not Equals		

84. Passare a **CERTIFICATO** e fare clic sulla freccia destra.

Standard
⇔- ■ 1
Carthader, Access
CHA
😋 Caco JP JPares
CambractH12
Carry-Recess
Q Discovery
Cogleyee/11
PermitAccess
🔐 Propulskan 🕤

85. Selezionare Nome alternativo soggetto.



86. Per il profilo AuthZ, selezionare Standard.

	Profiles	
		۵.
	◆- ■ '≡	ŵ- 5
cy Elements	🔚 Jake Posture Rode	
	🛄 finanty Group	
	Standard	R
o_IP_Phones		
4		
rision		
AuthZ Profil 🗢		
Select an item	15	

87. Selezionare Permit Access.



88. Selezionate Fatto (Done).



Questo è un esempio della regola:

1	OpenCHA /	Wester, Mill	ther	CHR
1	rtsihuk í	Weeken, 802.51 <== Network Access Authenticator/Hethod 802.04.5 MICHARY2 3		Provision
1	AllowRule if	Wireless_802.1X Radius:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name		PermitAccess

89. Individuare la regola predefinita per modificare PermitAccess in DenyAccess.



90. Per modificare la regola predefinita, fare clic su Modifica.



91. Passare al profilo AuthZ esistente di PermitAccess.



92. Selezionare Standard.



93. Selezionare **DenyAccess**.

Star	ndard
4.	
ě	CHA
ä	Contractivit2
	DenyAccess

94. Confermare che la regola predefinita disponga di DenyAccess se non vengono trovate corrispondenze.



95. Selezionate Fatto (Done).



Questo è un esempio delle regole principali richieste per il test e sono applicabili per uno scenario SSID singolo o SSID doppio.

OpenCWA	if	Wireless_MAB	then	CWA
PEAPrule	ť	(Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then	Provision
AllowRule	1	(Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name)	then	PermitAccess
Default	ife	o matches, then DenyAccess		

96. Fare clic su Salva.



97. Per configurare il server ISE con un profilo SCEP, selezionare **ISE > Administration > System > Certificates**.



98. In Operazioni certificato fare clic su Profili CA SCEP.



99. Fare clic su Add.



100. Immettere i seguenti valori per il profilo:

Nome: **mySCEP** (in questo esempio)URL: **https://***<ca-server>/***CertSrv/mscep/** (verificare la configurazione del server CA per l'indirizzo corretto).

EP Certificat	e Authority	
* Name	mySCEP	
Description		
* URL	https://10.10.10.10/certsrv/mscep/	Test Connectivity

101. Fare clic su Test connettività per verificare la connettività della connessione SCEP.



102. Questa risposta indica che la connettività del server è riuscita.



103. Fare clic su Invia.



104. Il server risponde che il profilo CA è stato creato correttamente.



105. Confermare che il profilo CA SCEP sia stato aggiunto.

SCEP CA Profiles			♦ ⊜ .
/Edit +Add XDelete		Show All	- 8
Name Name	Description	URL	CA Cert Name
MySCEP		https://10.10.10.10/certsrv/mscep	RFDemo-MSCE

Esperienza utente - Provisioning iOS

SSID doppio

In questa sezione vengono illustrati due SSID e viene descritto come connettersi al guest di cui eseguire il provisioning e come connettersi a una WLAN 802.1x.

Completare questi passaggi per effettuare il provisioning di iOS nello scenario con doppio SSID:

1. Sul dispositivo iOS, andare su **Reti Wi-Fi** e selezionare **DemoCWA** (configurato per aprire WLAN su WLC).



2. Aprire il browser Safari sul dispositivo iOS e visitare un URL raggiungibile (ad esempio, server Web interno/esterno). L'ISE vi reindirizza al portale. Fare clic su **Continue** (Continua).



3. Viene eseguito il reindirizzamento al portale per l'accesso.



4. Accedere con un account utente e una password di Active Directory. Installare il profilo CA quando richiesto.



5. Fare clic su Installa certificato protetto del server CA.



6. Fare clic su **Fine** una volta completata l'installazione del profilo.



7. Tornare al browser e fare clic su **Registra**. Prendere nota dell'ID dispositivo che contiene l'indirizzo MAC del dispositivo.



8. Per installare il profilo verificato, fare clic su Installa.



9. Fare clic su Installa.



10. Al termine del processo, il profilo WirelessSP conferma che il profilo è installato. Selezionate **Fatto (Done)**.



11. Accedere a **Reti Wi-Fi** e modificare la rete in **Demo1x**. Il dispositivo è ora connesso e utilizza TLS.

Settings Wi-Fi Netw	orks
Wi-Fi	
Choose a Network	
bibo	i 🕈 🧕
✓ Demo1x	۵ ج 🗎
DemoCWA	ş 📀
Netherstorm	4 🕈 🧕

12. In ISE, selezionare Operations > Authentications (Operazioni > Autenticazioni). Gli eventi mostrano il processo in cui il dispositivo è connesso alla rete guest aperta, passa attraverso il processo di registrazione con il provisioning del richiedente e viene consentito l'accesso dopo la registrazione.

A Home Operations	• Pol	cy •	Administration •						••
Authentications	e Endpo	ant Prote	ection Service	Alams 👖 Report	s Trouble	shoot			
Live Authentications									
谷 Add or Renove Columns 🕶	the Ref	resh					Refresh Every 3 secon	ds • Show	Latest 20 records * within [
Time	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:27:57.052 AM			paul	E8:06:80:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:27:21.714 AM			68:05:88:97:09:41	E8:05:08:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM	12				WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM		a	paul	E0:06:00:97:09:41	WLC	CWA	Any,Profiled:Apple-Pad	Pending	

13. Passare a ISE > Amministrazione > Gestione identità > Gruppi > Gruppi di identità degli endpoint > Dispositivi registrati. L'indirizzo MAC è stato aggiunto al database.

🛕 Home Operations 🔹 Policy 🔹 Admir 🔆 System 🙀 Identity Management	nistr N	ation 🔹	esource	es 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources		Identity Endpoint G Desc Parent Save Care Identit dentit	Source roup List nt Gro Name iption Group Res oints y Group Add AC Add S:06:88	e Sequences Settings t > RegisteredDevices RegisteredDevices Asset Registered Endpoints Identity Group set p Endpoints x Remove fiess 9:97:09:41 x

SSID singolo

In questa sezione viene descritto un singolo SSID e viene descritto come connettersi direttamente a una WLAN 802.1x, fornire nome utente e password di Active Directory per l'autenticazione PEAP, effettuare il provisioning tramite un account guest e riconnettersi a TLS.

Completare questi passaggi per eseguire il provisioning di iOS nello scenario SSID singolo:

1. Se si utilizza lo stesso dispositivo iOS, rimuovere l'endpoint dai dispositivi registrati.

Endpoint Group List > RegisteredDevices Endpoint Group					
* Name	RegisteredDevices				
Description [Asset Registered Endpoint				
Parent Group					
Save Rese	t				
 Endpoints 					
Identity Grou	p Endpoints				
add 🕂	×Remove •				
MAC Addr	e Remove Selected				
E8:06:88:	9 Remove All				

2. Sul dispositivo iOS, selezionare **Settings > Generals > Profiles** (Impostazioni > Generali > **Profili)**. Rimuovere i profili installati in questo esempio.



3. Per rimuovere i profili precedenti, fare clic su Rimuovi.





- 4. Connettersi direttamente a 802.1x con il dispositivo esistente (cancellato) o con un nuovo dispositivo iOS.
- 5. Connetti a Dot1x, immetti un nome utente e una password e fai clic su Partecipa.

Enter the password for "Demo1x" Cancel Enter Password Join				
Username pau	1			
Password •••••3				
Mode	Automatic >			

6. Ripetere i passaggi da 90 a 90 dalla sezione Configurazione ISE fino al completamento

dell'installazione dei profili appropriati.

 Per controllare il processo, selezionare ISE > Operations > Authentications. Nell'esempio viene mostrato il client connesso direttamente alla WLAN 802.1X quando viene attivato, disconnesso e riconnesso alla stessa WLAN con l'uso di TLS.

Live Authentications									
🚔 Add or Remove Columns 💌	😵 Rah	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03:593 AM		ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM	2	à	paul	E8:06:08:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

 Passare a WLC > Monitor > [MAC client]. Nel dettaglio del client, notare che il client si trova nello stato RUN, il relativo Data Switching è impostato su local e l'autenticazione è Central. Ciò vale per i client che si connettono a FlexConnect AP.

Live Authentications									
🙀 Add or Remove Columns 🔹	😵 Ref	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03:593 AM	2	ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM		ò	paul	E0.05.00.97.09.41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

Esperienza utente - Provisioning di Android

SSID doppio

In questa sezione vengono illustrati due SSID e viene descritto come connettersi al guest di cui eseguire il provisioning e come connettersi a una WLAN 802.1x.

Il processo di connessione per il dispositivo Android è molto simile a quello per un dispositivo iOS (singolo o doppio SSID). Tuttavia, una differenza importante è che il dispositivo Android richiede l'accesso a Internet per accedere a Google Marketplace (ora Google Play) e scaricare l'agente supplicant.

Completare questi passaggi per effettuare il provisioning di un dispositivo Android (come il Samsung Galaxy in questo esempio) nello scenario con doppio SSID:

1. Nel dispositivo Android, usare Wi-Fi per collegarsi a **DemoCWA** e aprire la WLAN guest.



2. Accettare tutti i certificati per collegarsi all'ISE.



3. Immettere un nome utente e una password nel portale guest per eseguire il login.



4. Fare clic su Registra. Il dispositivo tenta di raggiungere Internet per accedere a Google

Marketplace. Aggiungere eventuali regole aggiuntive all'ACL di pre-autenticazione (ad esempio, ACL-REDIRECT) nel controller per consentire l'accesso a Internet.

Inttps://market.androi O	×
Device Registration This device has not been registered. To register this device, please enter the Device ID (MAC Address format nonnexe enter A-F or a digt 0-10) and a description (optional). Please (this the "Register" button to Install and run the Cloco WI-FI Setup Assistant application. This application will inso ortificates and configures your device to use secure with network. Clicking the "Register" button will redirect you to an where you can download the Cloco WI-FI Setup Assistant application.	peed Log Cut Abo schools where it is fall all the necessary indroid market place,
Device 10 98.0C.82.40-31-A9 Description	

5. Google elenca Cisco Network Setup come app per Android. Fare clic su INSTALLA.



6. Accedere a Google e fare clic su INSTALL (INSTALLA).



7. Fare clic su OK.



8. Sul dispositivo Android, trovare l'app Cisco SPW installata e aprirla.



- 9. Verificare di aver ancora eseguito l'accesso al portale guest dal dispositivo Android.
- 10. Per avviare l'Assistente installazione Wi-Fi, fare clic su Start.



11. L'SPW Cisco inizia a installare i certificati.



12. Quando richiesto, impostare una password per l'archiviazione delle credenziali.



13. L'SPW Cisco restituisce un nome di certificato, che contiene la chiave utente e il certificato utente. Per confermare, fare clic su **OK**.

Certificate name					
Certificate name:					
paul					
Package contains One user key One user certificate					
ОК	Cancel				
Can	cel				

14. Cisco SPW continua e richiede un altro nome di certificato, che contiene il certificato CA. Immettere il nome **iseca** (in questo esempio), quindi fare clic su **OK** per continuare.

	111				
Certificate name					
Certificate name: iseca Package contains One CA certificate					
OK Cancel					
paul is installed. Cancel					

15. Il dispositivo Android è ora connesso.



Portale I miei dispositivi

My Devices Portal consente agli utenti di inserire nella blacklist i dispositivi registrati in precedenza in caso di smarrimento o furto di un dispositivo. Consente inoltre agli utenti di reinserirsi, se necessario.

Per mettere in blacklist un dispositivo, completare i seguenti passaggi:

1. Per accedere al portale I miei dispositivi, apri un browser, connettiti a https://iseserver:8443/mydevices (nota il numero di porta 8443) e accedi con un account AD.

CISCO My Devices Portal	
	Username paul Password
	Too br

2. Individuare il dispositivo in ID dispositivo e fare clic su **Lost?** per avviare la creazione della blacklist di un dispositivo.

Add a N	New Device	To add a device, please enter the Device ID (optional); then click submit to add the dev	0 (MAC Address) and a description rice.
Your Devic	* Device ID Description	Submit	•
State	Device ID D	exciption	Action
	E8:06:88:97:09:41		Edit Logi2 📓

3. Quando l'ISE chiede un avviso, fare clic su Yes (Sì) per procedere.



4. ISE conferma che il dispositivo è contrassegnato come perso.



5. Qualsiasi tentativo di connessione alla rete con il dispositivo registrato in precedenza è ora bloccato, anche se è installato un certificato valido. Questo è un esempio di un dispositivo in blacklist che non riesce ad autenticarsi:

Live Authentications		~~~~								
🙀 Add or Remove Columns 💌	😵 Raf	resh					Refresh E	very 3 seconds *	Show Latest 20 records	*
Time •	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event	
Mar 25,12 12:49:07.851 AM	•	ò	paul	E8:06:88:97:09:41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 25,12 12:40:59.057 AM	•	ò	68:06:08:97:09:41	EB-06-88-97-09-41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 95 10 10-40-54 197 AM				F0-04-00-00-01	WEC	Blacklet Access	Blacklet		Authentication field	

6. Un amministratore può passare a ISE > Amministrazione > Gestione identità > **Gruppi**, fare clic su **Gruppi di identità degli endpoint > Lista nera**, e vedere il dispositivo è in blacklist.

Identity Groups		Endp De Pare Save	Name escription int Group Res indpoints intity Group	Blacklist Blacklist Identity Group Blacklist Identity Group Bt
	3		+Add	×Remove +
	1		MAC Add	ress
	П		E8:06:88	:97:09:41
	11			

Per ripristinare un dispositivo in lista nera, completare i seguenti passaggi:

1. Dal portale I miei dispositivi, fare clic su **Reintegra** per il dispositivo.



2. Quando ISE chiede un avviso, fare clic su Sì per procedere.



3. ISE conferma che il dispositivo è stato ripristinato. Collegare il dispositivo reinstallato alla rete per verificare che sia autorizzato.



Riferimento - Certificati

ISE richiede non solo un certificato radice CA valido, ma anche un certificato valido firmato da CA.

Completare questa procedura per aggiungere, associare e importare un nuovo certificato CA attendibile:

1. Selezionare ISE > Administration > System > Certificates, fare clic su Local Certificates, quindi fare clic su Add.



2. Selezionare Genera richiesta di firma del certificato (CSR).

Local Cer	tificates			
/ Edit	+Add Export XDelete			
Friend Import Local Server Certificate				
	Generate Certificate Signing Request			
	Bind CA Certificate			

3. Immettere il **CN** del soggetto del certificato=<*ISE-SERVER nomehost.FQDN>*. Per gli altri campi, è possibile utilizzare il valore predefinito o i valori richiesti dall'impostazione della CA. Fare clic su **Invia**.

Local Certificates > Generate Certificate Signing Request Generate Certificate Signing Request			
Certificate			
* Certificate Subject * Key Length	CN=ise11-mnr.corp.rf-demo.com		
* Digest to Sign With	SHA-256 *		
Submit Cancel			

4. ISE verifica che il CSR sia stato generato.



5. Per accedere al CSR, fare clic sulle operazioni Richieste di firma certificato.



6. Selezionare il CSR creato di recente, quindi fare clic su Esporta.



7. ISE esporta il CSR in un file .pem. Per salvare il file sul computer locale, fare clic su **Salva file**, quindi su **OK**.



8. Individuare e aprire il file del certificato ISE con un editor di testo.

Downloads				_	
😋 🔾 - Paul N Downlo		👻 🚺 Sear	ch Downloads		- 2
Organize 👻 📄 Open 💌 Share with 🔹	•	New folder	800 -	- 🔟	•
☆ Favorites	-	Name *			
Nesktop		Save			
Dropbox		ise11mnrcorprfdemocomise11.pem			
' 🎉 Work		3			
🚺 Downloads					
Secent Places					

9. Copiare l'intero contenuto del certificato.



10. Connettersi al server CA e accedere con un account amministratore. Il server è una CA di Microsoft 2008 all'indirizzo https://10.10.10.10/certsrv (in questo esempio).

G • (ktps://10.10.10.10/certsrv/		. م	3 Cer
Windows Securit	y			×
Connecting to 1	0.10.10.10.			
				-
	administrator			
in the second				
	Domain: KFT7 Remember my credentials			
	_			
		OK	Cancel	

11. Fare clic su **Richiedi certificato**.



12. Fare clic su Richiesta avanzata di certificati.



13. Fare clic sulla seconda opzione per inviare una richiesta di certificato utilizzando un CMC con codifica Base 64 o



14. Incollare il contenuto del file del certificato ISE (.pem) nel campo Richiesta salvata, verificare che il modello di certificato sia **Server Web**, quindi fare clic su **Invia**.

Microsoft Certific	ate Services labsrv.corp.rf-demo.com				
Submit a Certificate Request or Renewal Request					
To submit a sav Saved Request	ved request to the CA, paste a base-64-encoded CN t box.				
Saved Request:					
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBc VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEB BQUAA4GBAKS+tyTCZiNKcXIygxHTW1epfDqWdoSZ 1/t65UI0KQAyBRUp21TpHf+o27eDTVwW83bCmbD1 osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM END CERTIFICATE				
Certificate Temp	late:				
	Web Server				
Additional Attrib	utes:				
Attributes:					
	Submit >				

15. Fare clic su Scarica certificato.



16. Salvare il file certnew.cer che verrà utilizzato in seguito per il binding all'ISE.

Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10.10?	Open Save V

17. Da Certificati ISE, passare a Certificati locali e fare clic su Add > Bind CA Certificate (Aggiungi > Certificato CA binding).
| 🛕 Home Operations 🔻 Policy 🔻 Adminis | tration 🔻 |
|--|--|
| 🔆 System 🦉 Identity Management 🛛 📷 🛙 | Network Resources 🛛 🛃 Web Portal Management |
| Deployment Licensing Certificates Loggin | g Maintenance Admin Access Settings |
| Certificate Operations | Local Certificates |
| Certificate Signing Requests Certificate Authority Certificates SCEP CA Profiles | Friend Import Local Server Certificate
Generate Self-Signed Certificate
Generate Certificate Signing Request |
| 🔅 OCSP Services | Bind CA Certificate |

 Individuare il certificato salvato nel computer locale nel passaggio precedente, abilitare entrambi i protocolli EAP e Management Interface (le caselle sono selezionate) e fare clic su Invia. ISE potrebbe richiedere alcuni minuti o più per riavviare i servizi.

Deployment Licensing Certificates Logo	ang Maintenance Admin Access Settings
Deployment Deeployment Decal Certificates Logging Manten Dertificate Operations Image: Certificates Bind CA S © Certificate Signing Requests Certificate Certificate © Certificate Authority Certificates Certificat * Certificat © OCSP Services Image: Certificates Image: Certificates Protocol Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Certificates Image: Certificate Signing Requests Image: Certificates Image: Certificates Image: Cer	ging Maintenance Admin Access Settings Local Certificates > Bind CA Signed Certificate Bind CA Signed Certificate Elind CA Signed Certificate Ecrtificate * Certificate File C\Users\Paul Nguyen\Downloads\certnew(4).cer Browse Friendly Name
	Override Policy Replace Certificate A certificate being imported may be determined to already exist in the syst certificate Selections for the certificate. Cancel Cancel

19. Tornare alla pagina iniziale della CA (https://CA/certsrv/) e fare clic su Scarica certificato CA, catena di certificati o CRL.



20. Fare clic su Scarica certificato CA.

Microsoft Active Directory Certificate Services - co				
Download a CA Certificate, Certificate Ch				
To trust certificates issued from this certification				
To download a CA certificate, certificate chair				
CA certificate:				
Current [corp-RFDEMO-CA]				
Encoding method:				
≪ DER C Base 64				
Download CA certificate				
Download latest base CRL				
Download latest delta CRL				

21. Salvare il file nel computer locale.

|--|

22. Con il server ISE in linea, andare su **Certificati**, quindi fare clic su **Certificati Autorità di certificazione**.



23. Fare clic su Import (Importa).



24. Cercare il certificato CA, abilitare l'opzione **Attendibilità per l'autenticazione client** (casella selezionata) e fare clic su **Invia**.



25. Confermare l'aggiunta del nuovo certificato CA attendibile.

🔆 System 🦉 Identity Management	Network Resource	es 🛛 🛃 Web Porta	al Managemer	
Deployment Licensing Certificates	Logging Maintenance	e Admin Access	Settings	
Certificate Operations	Certificate Au	Certificate Authority Certificates		
Certificate Signing Requests	/ Edit 🕂 I	Import Export	XDelete	
Certificate Authority Certificates	Friendly Na	ame		
SCEP CA Profiles	Corp-RFDE	corp-RFDEMO-CA#corp-RFDEMO-CA#00002		
👳 OCSP Services	ise11-mnr.	corp.rf-demo.com#ise	e11-mnr.corp	

Informazioni correlate

- Guida all'installazione dell'hardware di Cisco Identity Services Engine, versione 1.0.4
- <u>Cisco serie 2000 Wireless LAN Controller</u>
- <u>Cisco serie 4400 Wireless LAN Controller</u>
- <u>Cisco Aironet serie 3500</u>
- Guida all'installazione di Flex 7500 Wireless Branch Controller
- Personalizzazione del dispositivo Autenticazione unificata del dispositivo ed esperienza di accesso coerente
- BYOD wireless con Identity Services Engine
- Documentazione e supporto tecnico Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).