Bereitstellungsleitfaden für Wireless BYOD für FlexConnect

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten **Topologie** Geräteregistrierung und Komponentenbereitstellung Portal zur Registrierung von Ressourcen Portal zur Selbstregistrierung Authentifizierung und Bereitstellung Bereitstellung für iOS (iPhone/iPad/iPod) Bereitstellung für Android Dual-SSID Wireless BYOD-Selbstregistrierung Einzelne SSID Wireless BYOD-Selbstregistrierung **Feature-Konfiguration** WLAN-Konfiguration **FlexConnect AP-Konfiguration ISE-Konfiguration** Benutzerfreundlichkeit - Bereitstellung von iOS **Duale SSID Eine SSID** Benutzererlebnis - Bereitstellung von Android **Duale SSID** Geräteportal Referenz - Zertifikate Zugehörige Informationen

Einleitung

Mobilgeräte werden immer leistungsfähiger und beliebter bei Verbrauchern. Millionen dieser Geräte werden über Hochgeschwindigkeits-Wi-Fi an Privatnutzer verkauft, damit diese miteinander kommunizieren und zusammenarbeiten können. Die Verbraucher sind inzwischen an die Produktivitätssteigerung gewöhnt, die diese Mobilgeräte mit sich bringen, und möchten ihre persönliche Erfahrung mit in den Arbeitsbereich integrieren. Daraus ergeben sich die Funktionsanforderungen einer BYOD-Lösung (Bring Your Own Device) am Arbeitsplatz.

Dieses Dokument beschreibt die Bereitstellung der BYOD-Lösung in der Zweigstelle. Ein

Mitarbeiter stellt über sein neues iPad eine Verbindung zu einem SSID (Corporate Service Set Identifier) her und wird zu einem Portal zur Selbstregistrierung weitergeleitet. Die Cisco Identity Services Engine (ISE) authentifiziert den Benutzer über das Active Directory (AD) des Unternehmens und lädt ein Zertifikat mit einer eingebetteten iPad-MAC-Adresse und einem Benutzernamen auf das iPad herunter, zusammen mit einem Supplicant-Profil, das die Verwendung des Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) als Methode für die 802.1x-Konnektivität erzwingt. Basierend auf der Autorisierungsrichtlinie der ISE kann der Benutzer dann mithilfe von dot1x eine Verbindung herstellen und auf die entsprechenden Ressourcen zugreifen.

Die ISE-Funktionen in den Softwareversionen der Cisco Wireless LAN Controller-Software vor 7.2.110.0 unterstützten keine lokalen Switching-Clients, die über FlexConnect Access Points (APs) eine Verbindung herstellen. Version 7.2.110.0 unterstützt diese ISE-Funktionen für FlexConnect APs für lokales Switching und zentral authentifizierte Clients. Darüber hinaus bietet die mit ISE 1.1.1 integrierte Version 7.2.110.0 (ist jedoch nicht darauf beschränkt) folgende Funktionen der BYOD-Lösung für Wireless-Netzwerke:

- Erstellung von Geräteprofilen und Status
- Geräteregistrierung und Komponentenbereitstellung
- Integration privater Geräte (Bereitstellung von iOS- oder Android-Geräten)

Hinweis: Andere Geräte wie drahtlose PC- oder Mac-Laptops und Workstations werden zwar unterstützt, sind jedoch nicht in diesem Leitfaden enthalten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switches
- Cisco Wireless LAN (WLAN) Controller
- Cisco WLAN Controller (WLC) Softwareversion 7.2.110.0 und höher
- 802.11n APs im FlexConnect-Modus
- Cisco ISE Software Version 1.1.1 und höher
- Windows 2008 AD mit Zertifizierungsstelle
- DHCP-Server
- DNS-Server (Domain Name System)
- Network Time Protocol (NTP)
- Wireless-Client: Laptop, Smartphone und Tablet (Apple iOS, Android, Windows und Mac)

Hinweis: Wichtige Informationen zu dieser Softwareversion finden Sie in den

Versionshinweisen für Cisco Wireless LAN-Controller und Lightweight Access Points für Version 7.2.110.0. Melden Sie sich bei der Website Cisco.com an, um die neuesten Versionshinweise zu erhalten, bevor Sie Software laden und testen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Topologie

Um diese Funktionen ordnungsgemäß zu implementieren und zu testen, ist eine minimale Netzwerkeinrichtung erforderlich, wie in diesem Diagramm gezeigt:



Für diese Simulation benötigen Sie ein Netzwerk mit einem FlexConnect AP, einem lokalen/entfernten Standort mit lokalem DHCP, DNS, dem WLC und der ISE. Der FlexConnect-AP ist mit einem Trunk verbunden, um das lokale Switching mit mehreren VLANs zu testen.

Geräteregistrierung und Komponentenbereitstellung

Ein Gerät muss registriert werden, damit seine native Komponente für die 802.1x-Authentifizierung bereitgestellt werden kann. Basierend auf der richtigen Authentifizierungsrichtlinie wird der Benutzer auf die Gastseite umgeleitet und durch die Anmeldeinformationen des Mitarbeiters authentifiziert. Der Benutzer sieht die Seite zur Geräteregistrierung, auf der er nach seinen Geräteinformationen fragt. Anschließend wird mit der Gerätebereitstellung begonnen. Wenn das Betriebssystem für die Bereitstellung nicht unterstützt wird, wird der Benutzer zum Portal für die Bestandsregistrierung weitergeleitet, um das Gerät für den MAB-Zugriff (MAC Authentication Bypass) zu markieren. Wenn das Betriebssystem unterstützt wird, beginnt der

Registrierungsprozess und konfiguriert die native Komponente des Geräts für die 802.1x-Authentifizierung.

Portal zur Registrierung von Ressourcen

Das Portal zur Bestandsregistrierung ist Teil der ISE-Plattform, über die Mitarbeiter die Einbindung von Endgeräten über einen Authentifizierungs- und Registrierungsprozess initiieren können.

Administratoren können Ressourcen von der Seite mit den Endgerätidentitäten löschen. Jeder Mitarbeiter kann die von ihm registrierten Ressourcen bearbeiten, löschen und auf eine Blacklist setzen. Endgeräte, die auf einer Blacklist stehen, werden einer Identitätsgruppe auf einer Blacklist zugewiesen, und es wird eine Autorisierungsrichtlinie erstellt, um den Netzwerkzugriff durch Endgeräte auf einer Blacklist zu verhindern.

Portal zur Selbstregistrierung

Im CWA-Prozess (Central Web Authentication) werden Mitarbeiter zu einem Portal umgeleitet, in dem sie ihre Anmeldeinformationen eingeben, sich authentifizieren und die Details der Ressource eingeben können, die sie registrieren möchten. Dieses Portal wird als Self-Provisioning Portal bezeichnet und ähnelt dem Device Registration Portal. Es ermöglicht den Mitarbeitern, die MAC-Adresse sowie eine sinnvolle Beschreibung des Endpunkts einzugeben.

Authentifizierung und Bereitstellung

Wenn Mitarbeiter das Portal zur Selbstregistrierung auswählen, müssen sie eine Reihe gültiger Mitarbeiteranmeldeinformationen angeben, um mit der Bereitstellungsphase fortzufahren. Nach erfolgreicher Authentifizierung kann der Endpunkt in der Endpunktdatenbank bereitgestellt werden, und für den Endpunkt wird ein Zertifikat generiert. Über einen Link auf der Seite kann der Mitarbeiter den Supplicant Pilot Wizard (SPW) herunterladen.

Hinweis: Die neueste FlexConnect-Funktionsmatrix für BYOD finden Sie im Cisco Artikel zur <u>FlexConnect-Funktionsmatrix</u>.

Bereitstellung für iOS (iPhone/iPad/iPod)

Für die EAP-TLS-Konfiguration folgt die ISE dem Apple Over-the-Air (OTA)-Registrierungsprozess:

- Nach erfolgreicher Authentifizierung evaluiert die Evaluierungs-Engine die Richtlinien für die Client-Bereitstellung, wodurch ein Komponentenprofil erstellt wird.
- Wenn das Supplicant-Profil für die EAP-TLS-Einstellung verwendet wird, bestimmt der OTA-Prozess, ob die ISE selbstsignierte oder von einer unbekannten Zertifizierungsstelle signierte Zertifikate verwendet. Wenn eine der Bedingungen zutrifft, wird der Benutzer aufgefordert, das Zertifikat der ISE oder CA herunterzuladen, bevor der Registrierungsprozess beginnen

kann.

• Bei anderen EAP-Methoden sendet die ISE bei erfolgreicher Authentifizierung das endgültige Profil weiter.

Bereitstellung für Android

Aus Sicherheitsgründen muss der Android-Agent von der Android Marketplace-Website heruntergeladen werden und kann nicht über die ISE bereitgestellt werden. Cisco lädt eine Version des Assistenten für Veröffentlichungskandidaten über das Cisco Android Marketplace Publisher-Konto in den Android Marketplace hoch.

Dies ist der Android-Bereitstellungsprozess:

- 1. Cisco verwendet das Software Development Kit (SDK), um das Android-Paket mit der Erweiterung .apk zu erstellen.
- 2. Cisco lädt ein Paket in den Android Marketplace hoch.
- 3. Der Benutzer konfiguriert die Richtlinie bei der Client-Bereitstellung mit den entsprechenden Parametern.
- 4. Nach der Registrierung des Geräts wird der Endbenutzer an den Client-Bereitstellungsdienst weitergeleitet, wenn die 802.1x-Authentifizierung fehlschlägt.
- 5. Die Seite des Bereitstellungsportals enthält eine Schaltfläche, über die Benutzer zum Android Marketplace-Portal weitergeleitet werden, wo sie den SPW herunterladen können.
- 6. Der Cisco SPW wird gestartet und übernimmt die Bereitstellung der Komponente: SPW erkennt die ISE und lädt das Profil von der ISE herunter.SPW erstellt ein Zertifikat-/Schlüsselpaar für EAP-TLS.SPW führt einen SCEP-Proxy-Anforderungsaufruf (Simple Certificate Enrollment Protocol) an die ISE durch und empfängt das Zertifikat.SPW wendet die Wireless-Profile an.SPW löst eine erneute Authentifizierung aus, wenn die Profile erfolgreich angewendet werden.SPW wird beendet.

Dual-SSID Wireless BYOD-Selbstregistrierung

Dies ist der Prozess für die Selbstregistrierung von zwei SSID-Wireless-BYOD-Geräten:

- 1. Der Benutzer wird der Gast-SSID zugewiesen.
- 2. Der Benutzer öffnet einen Browser und wird zum ISE CWA-Gastportal weitergeleitet.
- 3. Der Benutzer gibt einen Benutzernamen und ein Kennwort für den Mitarbeiter in das Gastportal ein.
- 4. Die ISE authentifiziert den Benutzer und leitet ihn, basierend auf der Tatsache, dass es sich um einen Mitarbeiter und nicht um einen Gast handelt, auf die Gastseite für die Mitarbeiterregistrierung um.
- 6. Der Benutzer wählt "**Akzeptieren**" und beginnt mit dem Herunterladen und der Installation des SPW.
- 7. Die Komponente für das Gerät dieses Benutzers wird zusammen mit allen Zertifikaten bereitgestellt.

8. CoA tritt auf, und das Gerät ordnet es dem Unternehmens-SSID (CORP) zu und authentifiziert sich mit EAP-TLS (oder einer anderen für diesen Supplicant verwendeten Autorisierungsmethode).

Einzelne SSID Wireless BYOD-Selbstregistrierung

In diesem Szenario gibt es eine einzige SSID für den Unternehmenszugriff (CORP), die sowohl PEAP (Protected Extensible Authentication Protocol) als auch EAP-TLS unterstützt. Es ist keine Gast-SSID vorhanden.

Dies ist der Prozess für die Selbstregistrierung eines einzelnen SSID Wireless-BYOD-Geräts:

- 1. Der Benutzer ist CORP zugeordnet.
- 2. Der Benutzer gibt einen Benutzernamen und ein Kennwort für den Mitarbeiter in die Komponente für die PEAP-Authentifizierung ein.
- 3. Die ISE authentifiziert den Benutzer und stellt, basierend auf der PEAP-Methode, eine Autorisierungsrichtlinie zum Akzeptieren und Umleiten auf die Gastseite "Employee Device Registration" bereit.
- 4. Der Benutzer öffnet einen Browser und wird auf die Gastseite Employee Device Registration (Registrierung von Mitarbeitergeräten) weitergeleitet.
- 5. Die MAC-Adresse wird für die Geräte-ID auf der Gastseite für die Geräteregistrierung eingetragen. Der Benutzer gibt eine Beschreibung ein und akzeptiert die Nutzungsrichtlinien.
- Der Benutzer wählt "Akzeptieren" und beginnt mit dem Herunterladen und der Installation des SPW.
- 7. Die Komponente für das Gerät dieses Benutzers wird zusammen mit allen Zertifikaten bereitgestellt.
- 8. CoA tritt auf, und das Gerät weist die CORP-SSID erneut zu und authentifiziert sich mit EAP-TLS.

Feature-Konfiguration

Gehen Sie wie folgt vor, um mit der Konfiguration zu beginnen:

1. Achten Sie bei diesem Leitfaden darauf, dass die WLC-Version 7.2.110.0 oder höher ist.

	MONITOR MLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Monitor	Summary					
Summary Access Points Cisco CleanAir Statistics CDP	-1 1-1 1- CISCO	ss Points Supporte			D Series Wireless C	Controller
Clients	Controller Summa	iry		Re	gue Summary	
Multicast	Management IP Address	10.10.10.5		A	ctive Rogue APs	
	Software Version	7.2.104.16		A	ctive Rogue Clients	
	Field Recovery Image	1.0.0		A	dhoc Rogues	
	System Name	wic-11mm		R	ogues on Wired Net	work

2. Navigieren Sie zu **Security > RADIUS > Authentication**, und fügen Sie den RADIUS-Server dem WLC hinzu.

uludu cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDBA	сĸ
Security	RADIUS	Authentica	tion Serve	rs					
AAA General RADIUS Authentication Accounting Fallback	Call Stat Use AES MAC Del	ion ID Type ¹ Key Wrap Imiter	System Mi (Designed Hyphen	AC Address 1 for FIPS custome	rs and require	es a key wrap com	oliant RADIUS ser	rver)	
TACACS+ LDAP	Network User	Management	Server Index	Server Addre	ss Port	19	Sec	Admin Status	
MAC Filtering Disabled Clients User Login Policies	8	۲	1	10.10.10.60	1812	D	sabled	Enabled	

3. Fügen Sie die ISE 1.1.1 zum WLC hinzu:

Geben Sie einen freigegebenen Schlüssel ein.Legen Sie die Unterstützung für RFC 3576 auf Aktiviert fest.

MONITOR WLANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
RADIUS Authentication Serve	rs > Edit					
Server Index	1					
Server Address	10.10.10.60					
Shared Secret Format	ASCII :					
Shared Secret						
Confirm Shared Secret						
Key Wrap	(Designed for a state of the	r FIPS custom	ers and requires a l	key wrap complia	nt RADIU	S server)
Port Number	1812					
Server Status	Enabled :					
Support for RFC 3576	Enabled :					
Server Timeout	2 second	ds				
Network User	S Enable					
Management	S Enable					
IPSec	Enable					

4. Fügen Sie denselben ISE-Server wie einen RADIUS-Accounting-Server hinzu.

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANA		
RADIUS Accounti	ng Servers >	Edit				
Server Index	1					
Server Address	10.10	0.10.60				
Shared Secret Format	ASC	1I +				
Shared Secret	•••	•••				
Confirm Shared Secre	et	•••				
Port Number	1813					
Server Status	Enal	bled 1				
Server Timeout	2	seconds				
Network User	🗹 Er	nable				
IPSec		Enable				

 Erstellen Sie eine WLC-Pre-Auth-ACL, die Sie später in der ISE-Richtlinie verwenden können. Navigieren Sie zu WLC > Security > Access Control Lists > FlexConnect ACLs, und erstellen Sie eine neue FlexConnect ACL mit dem Namen ACL-REDIRECT (in diesem Beispiel).

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

6. In den ACL-Regeln muss der gesamte Datenverkehr von und zu der ISE sowie der Client-Datenverkehr während der Komponentenbereitstellung zugelassen werden.

Für die erste Regel (Sequenz 1):

Legen Sie "Quelle" auf "**Beliebig" fest**.Legen Sie IP (ISE-Adresse)/Netmask **255.255.255.255 fest**.Aktion auf **Zulassen** festlegen.

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 ‡		

Legen Sie für die zweite Regel (Sequenz 2) die Quell-IP-Adresse (ISE-Adresse)/-Maske 255.255.255.255 auf **Any (Beliebig) und die** Aktion auf **Permit (Zulassen)** fest.

Gene	ral									
Access	s List Name	ACL-RED	IR	ECT						
Seq	Action	Source IP/Mask	:	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	
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	1	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	

7. Erstellen Sie eine neue FlexConnect-Gruppe mit dem Namen Flex1 (in diesem Beispiel):

Navigieren Sie zur Registerkarte **FlexConnect Group > WebPolicies**.Klicken Sie im Feld WebPolicy ACL (WebPolicy-ACL) auf **Add (Hinzufügen**), und wählen Sie **ACL-REDIRECT** oder die zuvor erstellte FlexConnect-ACL aus.Bestätigen Sie, dass das Feld **WebPolicy Access Control Lists** ausgefüllt wird.



8. Klicken Sie auf Apply and Save Configuration.

WLAN-Konfiguration

Gehen Sie wie folgt vor, um das WLAN zu konfigurieren:

1. Erstellen Sie eine offene WLAN-SSID für das Beispiel mit zwei SSIDs:

Geben Sie einen WLAN-Namen ein: **DemoCWA** (in diesem Beispiel).Wählen Sie unter Status die Option **Enabled** (Aktiviert) aus.



2. Navigieren Sie zur Registerkarte Security (Sicherheit) > Layer 2 (Registerkarte Layer 2), und

legen Sie folgende Attribute fest:

Layer-2-Sicherheit: **Keine**MAC-Filterung: **Aktiviert** (Kontrollkästchen ist aktiviert)Schneller Übergang: **Deaktiviert** (Kontrollkästchen ist nicht aktiviert)

eneral	Security	QoS	Advanced					
Layer 2	Layer 3	AAA S	ervers					
	M.	MAC Filtering ²						
Fast Tran	M	AC Filterin	g <mark>2</mark> ✔					
Fast Tran	M	AC Filterin	g 2 ₽					
Fast Tran	Misition	AC Filterin	g 2 I ∕					

3. Wechseln Sie zur Registerkarte AAA-Server, und legen Sie folgende Attribute fest:

Authentifizierungs- und Kontoserver: aktiviertServer 1: </SE-IP-Adresse>

Layer 2	Layer 3	AAA Servers	
Select AAA	servers belo	ow to override use of default servers o	n this WLAN
Radius Ser	vers		
Radius S	Server Overw	rite interface Enabled	
Radius S	Server Overw	rite interface Enabled Authentication Servers Servers	Accounting Servers
Radius S	ierver Overw	rite interface Enabled Authentication Servers Enabled IP:10.10.10.60, Port:1812	Accounting Servers Enabled P:10.10.10.60, Port:1813
Radius S Server 1 Server 2	ierver Overw	rite interface Enabled Authentication Servers Enabled IP:10.10.10.60, Port:1812 None	Accounting Servers Enabled P:10.10.10.60, Port:1813 None

4. Blättern Sie von der Registerkarte **AAA-Server** nach unten. Vergewissern Sie sich unter "Authentication priority order for web-auth user", dass **RADIUS** für die Authentifizierung verwendet wird und die anderen nicht.



5. Wechseln Sie zur Registerkarte Erweitert, und legen Sie folgende Attribute fest:

AAA-Außerkraftsetzung zulassen: AktiviertNAC-Status: Radius NAC

Allow AAA Override	₽ Enabled	DHCP
Coverage Hole Date:Non	9 Enabled	DHCP Server Covered
Enable Secolon Timeout	Session Timeout (secs)	DHCP Addr. Assignment Require
Aironat 18	12 Enabled	Nanagement Frame Protection (NFF
Diagnostic Channel	C'Evabled	
Override Interface ACL	Prof. None R (Publ Rone R	1979 Class Protection . Optional
F2F Blacking Action	Constrined (A)	BTD9 Period (in beacan intervals)
Client Exclusion	C'Evabled	
Maximum Allowed		002.11.wh (1 - 200)
Clients *		882.1336/g/w (1 - 2993) [1
Static 3F Tunneling 🛤	C Enabled	NAC
Wi-Fi Direct Clients Folice	Doubled a	NAC State Radius NAC 💌
Recipces Allered	#*****	Load Balancing and Band Select
Chanty For AP Kullis	[244	Clarit Load Balancing

Hinweis: RADIUS Network Admission Control (NAC) wird nicht unterstützt, wenn sich der FlexConnect AP im getrennten Modus befindet. Befindet sich der FlexConnect-Access Point also im Standalone-Modus und wird die Verbindung zum WLC unterbrochen, werden alle Clients getrennt, und die SSID wird nicht mehr gemeldet.

6. Blättern Sie auf der Registerkarte Erweitert nach unten, und setzen Sie FlexConnect Local Switching auf **Aktiviert**.



7. Klicken Sie auf Apply and Save Configuration.



8. Erstellen Sie eine 802.1X-WLAN-SSID mit dem Namen **Demo1x** (in diesem Beispiel) für Einzel- und Dual-SSID-Szenarien.

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

 Navigieren Sie zur Registerkarte Security (Sicherheit) > Layer 2 (Registerkarte Layer 2), und legen Sie folgende Attribute fest:

Layer-2-Sicherheit: **WPA+WPA2**Schneller Übergang: **Deaktiviert** (Kontrollkästchen ist nicht aktiviert)Verwaltung von Authentifizierungsschlüsseln: 802.IX: **Aktivieren**

WLANs > E	dit 'Demo	1x'		
General	Security	QoS	Advand	ced
Layer 2	Layer 3	AAA S	ervers	
Layer 2	Security 😫 👖	WPA+WPA	2	•
	м	AC Filterin	9 2 🗖	
Fast Transit Over the D Reassociati	ion S on Timeout 20)		
WPA+WPA	2 Parameter	rs 🗖		
WPA2 P	olicy	5		
WPA2 E	ncryption	₩ AE	s 🗖	KIP
Authentica	ation Key Ma	nagemen	t	
802.1X	ع 🖓	nable		
CCKM	□ e	inable		
PSK	Π ε	inable		

10. Wechseln Sie zur Registerkarte **Erweitert**, und legen Sie folgende Attribute fest:

AAA-Außerkraftsetzung zulassen	: AktiviertNAC-Status: Radius NAC
--------------------------------	-----------------------------------

neral Security	QoS Advanced	
Allow AAA Override	F Enabled	DesC.P
Coverage Hole Detection	W Enabled	DHCP Server Covenide
Inable Session Timesult	(2000 Session Timeout (sess)	DHCP Addr. Assignment Required
kirunet III	9 Inabled	Nanagement Frame Protection (NFP)
Sagnastic Channel	C Enabled	
Iverride Interface ACL	IPv4 Note B IPv6 Note B	MPP Classit Protection # Optional (k)
OF Blocking Action	Disabled R	BTIN Period (in beacan intervalu)
Clerit Evolution 8	P Enabled Torecost Value (secs)	10 Hab 0 - 200
Racimum Alfored Dents	F	802.13b/g/s (1 - 250) 1
Natio IF Turneling M	T Enabled	NAC
Ki-Fi Direct Clients	(Destine) IN	NAC State Radius NAC •

11. Blättern Sie auf der Registerkarte **Advanced (Erweitert**) nach unten, und setzen Sie FlexConnect Local Switching auf **Enabled (Aktiviert)**.

FlexConnect	
FlexConnect Local Switching ²	☑ Enabled

12. Klicken Sie auf Apply and Save Configuration.



13. Vergewissern Sie sich, dass beide neuen WLANs erstellt wurden.

Мо	NITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WL	.ANs								Entries 1 - 5 of :
Cur	rent Filte	Nor	ne [Change	Filter] [Clear	Filter]		Create New	• 6	0
	WLAN ID	Туре	Profile Na	me		VLAN SSID		Admin Status	Security Policies
C		WLAS	85×			EG.H.		Disable	[[wra2][Aum(002.14)]
r.	2	wi_AN				ł		Enabled	[#PA2][Auth(PS2)]
	2	WLAN	Demo1x		C	Demo1x		Enabled	[WPA2][Auth(802.1X)]
	4	WLAN	DemoCWA		C	DemoCWA		Enabled	MAC Filtering
0	1	91,45	flex			føra		Orable	d Web-Auth

FlexConnect AP-Konfiguration

Führen Sie die folgenden Schritte aus, um den FlexConnect AP zu konfigurieren:

1. Navigieren Sie zu WLC > Wireless, und klicken Sie auf den Ziel-FlexConnect-AP.

	<u>W</u> LANs		WIRELESS
All APs			
Current Fil	lter		None
Number o	f APs		2
AP Name		AF	9 Model
Site-B-Flex	AP	AI	R-LAP1262N-A-K
	den -		

2. Klicken Sie auf die Registerkarte FlexConnect.



3. Aktivieren Sie VLAN Support (Kontrollkästchen ist aktiviert), legen Sie die Native VLAN ID fest, und klicken Sie auf VLAN Mappings.

VLAN Support	V	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Config	ured

4. Legen Sie die VLAN-ID für die SSID für das lokale Switching auf 21 (in diesem Beispiel) fest.

<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY
> Site-B-	FlexAP > VLA	N Mapping	S
e	Site-B-FlexAP		
dio MAC	e8:04:62:0a:68:8	D	
WLAN Id SSID			VLAN ID
Demo1x			21
DemoCW/	4		21
	WLANS > Site-B- dio MAC SSID Demo1x DemoCW/	WLANS CONTROLLER > Site-B-FlexAP VLA e Site-B-FlexAP dio MAC e8:04:62:0a:68:80 SSID Demo1x DemoCWA DemoCWA	WLANS CONTROLLER WIRELESS > Site-B-FlexAP > VLAN Mapping e Site-B-FlexAP dio MAC e8:04:62:0a:68:80 SSID Demo1x DemoCWA DemoCWA

5. Klicken Sie auf Apply and Save Configuration.

ISE-Konfiguration

Gehen Sie wie folgt vor, um die ISE zu konfigurieren:

1. Melden Sie sich beim ISE-Server an: <https://ise>.



2. Navigieren Sie zu Administration > Identity Management > External Identity Sources.



3. Klicken Sie auf Active Directory.



4. Auf der Registerkarte Verbindung:

Fügen Sie den Domänennamen **corp.rf-demo.com (**in diesem Beispiel) hinzu, und ändern Sie den Standardnamen des Identitätsspeichers in **AD1**.Klicken Sie auf **Konfiguration speichern**.Klicken Sie auf **Join** (Teilnehmen), und geben Sie den Benutzernamen und das Kennwort für das AD-Administratorkonto an, die für die Teilnahme erforderlich sind.Der Status muss grün sein. Aktivieren Sie **Verbunden mit**: (Kontrollkästchen ist aktiviert).

connection	Advanced S	Settings	Groups	Attr	ibutes		
		* Do	main Name	corp.rf-de	mo.com		
		* Identity	Store Name	AD1			
ne or more nodes	may be select	ted for Join	or Leave oper	rations. If	a node is join	ed then a lear	ve operation is
onnection.	may be selec	ted for Join	or Leave oper	rations. If	a node is join	ed then a lea	ve operation is
ne or more nodes onnection. 약을 Join 약을 Leave	may be selec	ted for Join	or Leave oper	rations. If	a node is join	ed then a lea	ve operation is
onnection. 양글 Join 약을 Leave	may be selec e <u>e</u> Test Co	ted for Join	ISE Node Ro	nations. If	a node is join tatus	ed then a lea	ve operation is

5. Durchführen eines einfachen Verbindungstests mit dem AD bei einem aktuellen Domänenbenutzer.

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

6. Wenn die Verbindung mit dem AD erfolgreich hergestellt wurde, wird in einem Dialogfeld bestätigt, dass das Kennwort richtig ist.



7. Navigieren Sie zu Administration > Identity Management > External Identity Sources:

Klicken Sie auf **Zertifikatauthentifizierungsprofil**.Klicken Sie auf **Hinzufügen**, um ein neues Zertifikatauthentifizierungsprofil (Certificate Authentication Profile, CAP) zu erstellen.

CISCO Identity Services Engine	
🍐 Home Operations 🔻 Policy 🔻 Admir	istration 🔻
🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web Portal Manage
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
∲-	In day Design Ma
Certificate Authentication Profile	Eait MAD L'Dupicate
2 Active Directory	Name V
🚞 LDAP 💿	
California RADIUS Token	
RSA SecurID	

8. Geben Sie den Namen **CertAuth** (in diesem Beispiel) für die CAP ein. Wählen Sie als Principal Username X509 Attribute den **Common Name aus,** und klicken Sie dann auf **Submit (Senden)**.

* Name	CertAuth	
Description		
Principal Username X509 Attribute	Common Name	Ŧ
Perform Binary Certificate Comp	arison with Certificate retrieved	from LDAP or Active Directory

9. Bestätigen Sie, dass die neue GAP hinzugefügt wird.

CISCO Identity Services Engine	
💧 Home Operations 🔻 Policy 🔻 Admini	stration 🔻
🔆 System 🦉 Identity Management 📰 I	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	□ Name
🚞 LDAP 🛞	Certiesen
RADIUS Token ()	
E RSA SecurID 💿	

10. Navigieren Sie zu Administration > Identity Management > Identity Source Sequences, und klicken Sie auf Add .

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	
/ Edit Add D Duplicate X Delete	
Name 🐨	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. Geben Sie der Sequenz den Namen TestSequence (in diesem Beispiel).

cisco Id	entity Services Engine
💧 Home	Operations Policy Administration
🔆 System	Veb Portal Mana
Identities (Groups External Identity Sources Identity Source Sequences Settings
Identity Source Seq Identity Sou ✓ Identity So	uences List > New Identity Source Sequence rce Sequence urce Sequence
* Name	TestSequence
Description	
 Certificate 	e Based Authentication

12. Blättern Sie nach unten zu Zertifikatbasierte Authentifizierung:

Aktivieren **Sie die Option Zertifikatauthentifizierungsprofil auswählen** (Kontrollkästchen ist aktiviert).Wählen Sie **CertAuth** (oder ein anderes zuvor erstelltes CAP-Profil) aus.

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

13. Blättern Sie nach unten zur Authentifizierungssuchliste:

AD1 von "Verfügbar" in "Ausgewählt" verschieben.Klicken Sie auf die Schaltfläche Nach oben, um AD1 zur obersten Priorität zu verschieben.

 Authentication Search List 	
A set of identity sources that will be accesse	d in sequence until first authentication succeeds
Available	Selected
	Internal Users
×	

14. Klicken Sie zum Speichern auf Senden.



15. Bestätigen Sie, dass die neue Identitätsquellensequenz hinzugefügt wird.

CISCO Identity Services Engine		
🛕 Home Operations 🔹 Policy 🔹 Administr	ation 🔹	
🔆 System 🛛 😤 Identity Management 🖉 Net	twork Resources 🚯 Web Portal Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Identity Source Sequence		
/ Edit		
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

16. Verwenden Sie AD, um das Portal "Meine Geräte" zu authentifizieren. Navigieren Sie zu ISE > Administration > Identity Management > Identity Source Sequence, und bearbeiten Sie MyDevices_Portal_Sequence.

🔆 System 🛛 餐 Identity Man	agement	Netwo	ork Resources 🛛 🛃 Web
Identities Groups External	Identity Sources	Ide	ntity Source Sequences
dentity Source Sequence			
mental and an and and and and and and and and			
,			
/ Edit -Add Duplicate	XDelete		
/ Edit -Add Duplicate	XDelete	•	Description
/ Edit + Add Duplicate	XDelete	-	Description A Built-in Identity Sequence
Edit Add Duplicate Name Guest_Portal_Sequence MyDevices_Portal_Sequence	XDelete	•	Description A Built-in Identity Sequence A Built-in Identity Sequence

17. Fügen Sie **AD1** zur Liste "Ausgewählt" hinzu, und klicken Sie auf die Schaltfläche "Nach oben", um AD1 zur obersten Priorität zu verschieben.



18. Klicken Sie auf Speichern.



19. Bestätigen Sie, dass die Identity Store-Sequenz für MyDevices_Portal_Sequence AD1 enthält.



20. Wiederholen Sie die Schritte 16-19, um AD1 für Guest_Portal_Sequence hinzuzufügen, und klicken Sie auf **Save**.



21. Bestätigen Sie, dass Guest_Portal_Sequence AD1 enthält.

	Name	Description	Identity Stores
Ð	Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
100			

22. Um den WLC dem Netzwerkzugriffsgerät (WLC) hinzuzufügen, navigieren Sie zu Administration > Network Resources > Network Devices, und klicken Sie auf Add.

cisco Identity Services Engine			
A Home Operations Policy A	dministration	4. Web Portal Management	
Network Device Groups	External RADIUS Servers	RADIUS Server Sequences	
Network Devices	Network Devic	es	
(• . ∉•	P / Edit - Add	Duplicate	•
Network Devices Default Device	Name	 IP/Mask Location 	n

23. Fügen Sie den WLC-Namen, die IP-Adresse, die Subnetzmaske usw. hinzu.

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

24. Navigieren Sie zu Authentifizierungseinstellungen, und geben Sie den gemeinsamen Schlüssel ein. Dies muss mit dem gemeinsamen geheimen Schlüssel des WLC-RADIUS übereinstimmen.

	 Authentication Setting)S		
		Enable Authentication Settings		
		Protocol	RADIUS	
		 Shared Secret 	•••••	Show
		Enable KeyWrap		
		 Key Encryption Key 		Show
		* Message Authenticator Code Key		Show
		Key Input Format	ASCII HEXADECIN	1AL
	SNMP Settings			
	 SGA Attributes 			
Sub	mit Cancel			

- 25. Klicken Sie auf Senden.
- 26. Navigieren Sie zu ISE > Policy > Policy Elements > Results.

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

27. Erweitern Sie **Ergebnisse** und **Autorisierung**, klicken Sie auf **Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**, um ein neues Profil anzuzeigen.

CISCO Identity Services Engine	6	1				0
🛕 Home Operations 🔻 Policy 🔻	Adminis	tration	•			
Authentication S Authorization	🛃 Pr	ofiling	2	Posture	Client	t Provisioning
Dictionaries Conditions Results						
Results		Star	ndard	Author	ization Pro	files
 	<u>م</u> ڇ	/	Edit	Add	Duplicate	XDelete
Authentication		H	Riacklik	t Access		
Authorization		n	Cisco 1	P Phone	e .	
 Authorization Profiles 			Contra	HV12		
Slacklist_Access			DenvA	COESS		

28. Geben Sie diesem Profil folgende Werte:

Name: CWA

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

Web-Authentifizierung aktivieren (Kontrollkästchen ist aktiviert):

Web-Authentifizierung: **zentralisiert**ACL: **ACL-REDIRECT** (ACL-**REDIRECT** muss mit dem Namen der vorauthentifizierten WLC-ACL übereinstimmen.)Umleitung: **Standard**

 Common Tasks 							
DACL Name							
ULAN VLAN							
Voice Domain Permissio	n						
Veb Authentication	Centralized	٣	ACL ACL	-REDIRECT	Redirect	Default	¥

29. Klicken Sie auf **Senden**, und bestätigen Sie, dass das CWA-Autorisierungsprofil hinzugefügt wurde.



30. Klicken Sie auf Hinzufügen, um ein neues Autorisierungsprofil zu erstellen.



31. Geben Sie diesem Profil folgende Werte:

Name: Provision

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

Web-Authentifizierung aktivieren (Kontrollkästchen ist aktiviert):

Wert der Webauthentifizierung: Bereitstellung von Komponenten

 Common Tasks 					
DACL Name					
U VLAN					
Voice Domain Permission	Voice Domain Permission				
Veb Authentication	Centralized *	ACL			
	Centralized				
Auto Smart Port	Device Registration				
Posture Discovery					
Hiter-ID	Supplicant Provisioning				
	9				

ACL: **ACL-REDIRECT** (ACL-**REDIRECT** muss mit dem Namen der vorauthentifizierten WLC-ACL übereinstimmen.)

 Common Tasks 			
DACL Name			
ULAN VLAN			
Voice Domain Permission			
☑ Web Authentication	Supplicant Provisioning *	ACL	ACL-REDIRECT
C Auto Smort Port			

32. Klicken Sie auf **Senden**, und bestätigen Sie, dass das Berechtigungsprofil "Bereitstellen" hinzugefügt wurde.



33. Blättern Sie in Results (Ergebnisse) nach unten, erweitern Sie **Client Provisioning**, und klicken Sie auf **Resources (Ressourcen)**.

🛕 Home Operations 🔻 Policy 🔻
Authentication Solution
Dictionaries Conditions Results
Results
∲• ≣ ≡
Authentication
Authorization
Profiling
Posture
Client Provisioning
Elesources ⊕ Security Group Access

34. Wählen Sie Native Supplicant Profile aus.



35. Geben Sie dem Profil den Namen WirelessSP (in diesem Beispiel).

tive Supplicant Profi	le
* Name	WirelessSP
Description	

36. Geben Sie folgende Werte ein:

Verbindungstyp: **Wireless**SSID: **Demo1x** (dieser Wert stammt aus der WLC 802.1x-WLAN-Konfiguration)Zulässiges Protokoll: **TLS**Schlüssellänge: **1024**

* Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demoix
		Security	WPA2 Enterprise +
* Allowed Protocol	PEAP		v
 Optional Settings 	TLS PEAP	ę	2
Submit Cancel			

- 37. Klicken Sie auf Senden.
- 38. Klicken Sie auf Speichern.

* Allowed Protocol	TLS	•
* Key Size	1024	
Save Reset		

39. Bestätigen Sie, dass das neue Profil hinzugefügt wurde.

Edit 🖶 Add 👻 🔂 Duj	olicate X Delete
Name	Туре
Revenue and	
Wireless	NativeSPProfile

40. Navigieren Sie zu Richtlinie > Client-Bereitstellung.



41. Geben Sie die folgenden Werte für die Bereitstellungsregel von iOS-Geräten ein:

Regelname: iOSIdentitätsgruppen: Alle

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

Betriebssysteme: Mac iOS Alle

Operating System Grou	ips
	Q
∲•	ŵ.
Android	
Mac OSX	
Mac iOS All	
🚞 Windows All	۲

Ergebnisse: WirelessSP (dies ist das zuvor erstellte Native Supplicant-Profil)

ther Conditions	Results		
	then Result 🕀 🦣		

Navigieren Sie zu Ergebnisse > Assistentenprofil (Dropdown-Liste) > WirelessSP.



WizardProfile	
	Q
◆- ■ '≣	<u>ن</u>
Clear Selection	
Wireless	

42. Bestätigen Sie, dass das iOS-Bereitstellungsprofil hinzugefügt wurde.

			Rule Name	I	Identity G	iroups		Operating System	ms		Other Conditions		Results	
1	2	٠	iOS	If [Any	\$	and	Mac IOS All	\diamond	and	Condition(s)	\$ then	WrelessSP	\diamond

43. Suchen Sie auf der rechten Seite der ersten Regel die Dropdown-Liste "Aktionen", und wählen Sie **Unten (**oder darüber) **Duplizieren**.



44. Ändern Sie den Namen der neuen Regel in Android.



45. Ändern Sie das Betriebssystem auf Android.



- 46. Lassen Sie die anderen Werte unverändert.
- 47. Klicken Sie auf Speichern (linker unterer Bildschirm).



48. Navigieren Sie zu ISE > Policy > Authentication.



49. Ändern Sie die Bedingung, sodass sie Wireless_MAB enthält, und erweitern Sie Wired_MAB.



50. Klicken Sie auf die Dropdown-Liste Bedingungsname.



51. Wählen Sie Wörterbücher > Zusammengesetzte Bedingung aus.



52. Wählen Sie Wireless_MAB aus.



53. Klicken Sie rechts neben der Regel auf den Pfeil, um sie zu erweitern.



54. Wählen Sie diese Werte aus der Dropdown-Liste aus:

Identitätsquelle: **TestSequence** (dies ist der zuvor erstellte Wert)Wenn Authentifizierung fehlgeschlagen ist: **Ablehnen**Wenn Benutzer nicht gefunden wird: **Fortfahren**Wenn der Prozess fehlgeschlagen ist: **Löschen**

use	TestSequence 🗢
	Identity Source TestSequence 📀
	Options
	If authentication failed Reject
ribula	If user not found Continue
	If process failed Drop 💌

55. Wechseln Sie zur Dot1X-Regel, und ändern Sie die folgenden Werte:



	pound Condition	
		م
4.	· 🔳 🗉 🛛	÷
	Wired_MAB	
	Wireless_MAB	
	Wired_802.1X	
ш. 1	Wireless_802.1X dm	
•	switch_Local_Web_Authenti	cation
	WLC_Web_Authentication	
If [Wired_802.1X	allo
al	Add All Conditions B	elow t
	Condition Name	

Zustand: Wireless_802.1X

Identitätsquelle: TestSequence

Identity Source TestSequence	se for authe			
Options	Identity Source List			
If authentication failed Reject				
If user not found Reject	[م			
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. Klicken Sie auf Speichern.



57. Navigieren Sie zu ISE > Policy > Authorization.


58. Die Standardregeln (z. B. Black List Default, Profiled und Default) sind bereits ab der Installation konfiguriert. Die ersten beiden Regeln können ignoriert werden. Die Standardregel wird zu einem späteren Zeitpunkt bearbeitet.

st Matche	d Rule Applies +		
Exception	s (0)		
Standard			
State	is Rule Name	Conditions (identity groups and other conditions)	Permissions
	Black List Default	if Blacklist	then Blacklist_Access

59. Klicken Sie rechts neben der zweiten Regel (Cisco IP-Telefone mit Profil) auf den Abwärtspfeil neben "Bearbeiten", und wählen Sie **Neue Regel darunter einfügen aus**.



Eine neue Standardregelnummer wird hinzugefügt.

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

60. Ändern Sie den Regelnamen von der Standardregelnummer in **OpenCWA**. Diese Regel initiiert den Registrierungsprozess im offenen WLAN (Dual-SSID) für Benutzer, die zum Gastnetzwerk kommen, um Geräte bereitstellen zu lassen.



61. Klicken Sie auf das Pluszeichen (+) für Bedingung(en), und klicken Sie auf Vorhandene Bedingung aus Bibliothek auswählen.

Cisco-IP-Phone		then Cisco_IP_Pho	
f Any \diamondsuit and	Select Condition	then AuthZ Pro	
n no matches, then Perm	Select Exis	ting Condition from Library 🕧 or 🤇 Create	

62. Wählen Sie Zusammengesetzte Bedingungen > Wireless_MAB aus.

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 5	
	1	
Select Condition	h	
Add All Conditions B		
Condition Name		
Select Condition		

63. Klicken Sie im AuthZ-Profil auf das Pluszeichen (+), und wählen Sie Standard aus.

	Profiles	
		P
licy Elements	(d-) :	-
	🚞 Inline Posture Node	۲
	Carlor Security Group	۲
	Standard 🕞	۲
rmissions		
icklist_Access		
co_IP_Phones		
AuthZ Profil 👄		
Select an item	○ - +	

64. Wählen Sie den Standard-CWA aus (dies ist das zuvor erstellte Autorisierungsprofil).



65. Bestätigen Sie, dass die Regel mit den richtigen Bedingungen und Autorisierungen hinzugefügt wurde.



66. Klicken Sie Fertig (auf der rechten Seite der Regel).



67. Klicken Sie rechts neben der gleichen Regel auf den Abwärtspfeil neben Bearbeiten, und wählen Sie **Neue Regel darunter einfügen aus**.



68. Ändern Sie den Regelnamen von Standardregelnummer in **PEAPrule** (in diesem Beispiel). Diese Regel gilt für PEAP (wird auch für ein Einzel-SSID-Szenario verwendet), um zu prüfen, ob die 802.1X-Authentifizierung ohne Transport Layer Security (TLS) erfolgt und die Bereitstellung der Netzwerkkomponenten mit dem zuvor erstellten Bereitstellungs-Autorisierungsprofil initiiert wurde.

🖉 🗹 OpenCWA	if Wireless_MAB	then CWA
💉 🔽 🔹 Standard Rule 1	f Any 💠 and Condition(s)	then Auth2 Profil

69. Ändern Sie die Bedingung in Wireless_802.1X.

Condition(s)	- then AuthZ Profil	
Add All Conditions Belo	w to Library	
Condition Name	Expression	
Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	- ∰•

70. Klicken Sie auf das Zahnrad-Symbol auf der rechten Seite der Bedingung, und wählen Sie **Attribut/Wert hinzufügen aus**. Dies ist eine 'und'-Bedingung, keine 'oder'-Bedingung.



71. Suchen Sie nach und wählen Sie Netzwerkzugriff aus.

	Dictionaries
	٩
	🔶 📃 📜 🛞 🖓 🖓
os and other conditions)	A 1997
	-
then	
then	
then	
Condition(s)	
tAccess	
Condition Name Expression	-
Wireless_802.1X 📀 Radius:Service-Type Ei	Network Access
Select Attribute	

72. Wählen Sie AuthenticationMethod aus, und geben Sie die folgenden Werte ein:



Authentifizierungsmethode: Equals

Network Access:Au🛇	· ·
	Equals Not Equals

Wählen Sie MSCHAPV2 aus.



Dies ist ein Beispiel für die Regel. Stellen Sie sicher, dass die Bedingung ein AND ist.

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

73. Wählen Sie in AuthZ Profile (AuthZ-Profil) **Standard > Provision (**dies ist das zuvor erstellte Autorisierungsprofil) aus.

then	AuthZ Profil	Done
	Select an item 📀	- +

Standard	ž -
	و م
∲- ■ '≣	ŵ.
and the second se	
Se Provision	
$\mathbf{\hat{v}}$	

74. Klicken Sie auf Fertig.



75. Klicken Sie rechts neben der PEAP-Regel auf den Abwärtspfeil neben Bearbeiten, und wählen Sie **Neue Regel darunter einfügen aus**.



76. Ändern Sie den Regelnamen von Standardregelnummer in **Zulassen** (in diesem Beispiel). Diese Regel wird verwendet, um den Zugriff auf registrierte Geräte mit installierten Zertifikaten zu ermöglichen.



77. Wählen Sie unter Bedingung(en) die Option Zusammengesetzte Bedingungen aus.

		P
	∲- ■ '≣	1/@+
ant Dravisioning	Simple Conditions	۲
	Compound Conditions	A.
	Time and Date Conditions	82
twork Access:Authentica:		
twork Access:Authenticat Condition(s)		h

78. Wählen Sie Wireless_802.1X aus.



79. Fügen Sie ein AND-Attribut hinzu.

- then	
w to Library	
Expression	
Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	B
	then then

80. Klicken Sie auf das Zahnrad-Symbol auf der rechten Seite der Bedingung, und wählen Sie Attribut/Wert hinzufügen aus.



81. Suchen Sie nach und wählen Sie Radius aus.

			Dictionaries	
	10		◆• ■ 'E	
Client Provisioning 🔄 Securi	ty Group Access	- 3	Citers	1
			Caco-MEDM	
		three	Caso-selectory	
		then	🚞 aesace	
		then	🔛 IndPoints	
	thread		🔛 duest	
etwork access: Authenticationme	thod	then	🔛 Admithydrouge	
Wireless 802.1X Network Acce	ss:A 🗢		🔛 Internal.teer	
1			Alcosoft 🧱	
Condition Name	Expression		Entwork Access	AND V
			🚞 Radius	
Wireless_802.1X 📀	Radius:Service-1	Type E/	Sectors 1	2
¢	Select Attrib	ute 🤇		O

82. Wählen Sie Calling-Station-ID-[31].



83. Wählen Sie Gleich.

Radius:Service-Type EQUALS Fran	ned AND Radius:NAS	S-Port
Radius:Calling-Statio	*	O
Equi	Equals	

84. Gehen Sie zu **ZERTIFIKAT**, und klicken Sie auf den Pfeil nach rechts.

Standard
⇔- ≣ '≣
Carthadan, Access
CHA
😋 Caco, JP JPares
Caretractivit2
Carty-Rocass
Ca Discovery
Ca Englisyeer/11
PermitAccess
😋 Provincen 🖸

85. Wählen Sie einen alternativen Antragstellernamen aus.



86. Wählen Sie als AuthZ-Profil die Option Standard aus.

	Profiles		
		٩	
	◆- ■ '≡	ŵ.,	
Elements	🔜 Julie Posture Node		
,	📒 Incety Group		
	Standard	R	
_IP_Phones		0	
sion			
AuthZ Profil 🗢			
Select an item	4		

87. Wählen Sie **Zugriff zulassen aus**.



88. Klicken Sie auf Fertig.



Dies ist ein Beispiel für die Regel:

I	OperCHA	Weden, Mill	The second	CHR
1	15thub	Intelest, 802 5X Intel Nativoli Access Authenticator/Hethod 803463 Https://www.access.authenticator/Hethod		Provision
1	AllowRule	Wireless_802.1X Radius:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	then	PermitAccess

89. Suchen Sie die Standardregel, um PermitAccess in DenyAccess zu ändern.



90. Klicken Sie auf Bearbeiten, um die Standardregel zu bearbeiten.



91. Wechseln Sie zum vorhandenen AuthZ-Profil von PermitAccess.



92. Wählen Sie Standard aus.



93. Wählen Sie Zugriff verweigern aus.

Standard	
↔• ■ '≡	
Cast	
Caso, JP , Phones Contractivit2	
Canton DenyAccess	

94. Vergewissern Sie sich, dass die Standardregel 'DenyAccess' enthält, wenn keine Übereinstimmungen gefunden werden.



95. Klicken Sie auf Fertig.



Dies ist ein Beispiel für die wichtigsten Regeln, die für diesen Test erforderlich sind. Sie gelten entweder für ein Einzel-SSID- oder ein Dual-SSID-Szenario.

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

96. Klicken Sie auf Speichern.



97. Navigieren Sie zu ISE > Administration > System > Certificates, um den ISE-Server mit einem SCEP-Profil zu konfigurieren.



98. Klicken Sie in Certificate Operations (Zertifikatvorgänge) auf SCEP CA Profiles (SCEP-Zertifizierungsstellenprofile).



99. Klicken Sie auf Hinzufügen.



100. Geben Sie folgende Werte für dieses Profil ein:

Name: **mySCEP** (in diesem Beispiel)URL: **https://**<*ca-server*>/**CertSrv/mscep/** (Die richtige Adresse finden Sie in der Konfiguration des Zertifizierungsstellen-Servers.)

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

101. Klicken Sie auf Verbindung testen, um die Verbindung der SCEP-Verbindung zu testen.



102. Diese Antwort zeigt, dass die Serververbindung erfolgreich ist.



103. Klicken Sie auf Senden.



104. Der Server antwortet, dass das CA-Profil erfolgreich erstellt wurde.



105. Bestätigen Sie, dass das SCEP-CA-Profil hinzugefügt wurde.

SCEP CA Profiles			
boor orritones			🥹 🏭 🗸
/Edt +Add XDelete		Show All	- 8
Name Name	Description	URL	CA Cert Name
MySCEP		https://10.10.10.10/certsrv/mscep	RFDemo-MSCE

Benutzerfreundlichkeit - Bereitstellung von iOS

Duale SSID

In diesem Abschnitt wird die duale SSID behandelt. Außerdem wird beschrieben, wie Sie eine Verbindung mit dem bereitzustellenden Gast und mit einem 802.1x-WLAN herstellen.

Gehen Sie wie folgt vor, um iOS im Szenario mit zwei SSIDs bereitzustellen:

1. Wechseln Sie auf dem iOS-Gerät zu **Wi-Fi Networks**, und wählen Sie **DemoCWA** (konfiguriert als offenes WLAN auf dem WLC) aus.

Settings Wi-Fi Networ	'ks
Wi-Fi	
Choose a Network	
bibo	47 😣
Demo1x	ی ج 🔒
✓ DemoCWA	÷ 🜔
Netherstorm	4 7 0
Other	>
Ask to Join Networks	ON
Known networks will b	e joined

 Öffnen Sie den Safari-Browser auf dem iOS-Gerät, und rufen Sie eine erreichbare URL auf (z. B. einen internen/externen Webserver). Die ISE leitet Sie zum Portal weiter. Klicken Sie auf Continue (Weiter).



3. Sie werden zur Anmeldung zum Gastportal weitergeleitet.



4. Melden Sie sich mit einem AD-Benutzerkonto und -Kennwort an. Installieren Sie das Zertifizierungsstellenprofil, wenn Sie dazu aufgefordert werden.



5. Klicken Sie auf Vertrauenswürdiges Zertifikat des Zertifizierungsstellenservers installieren.



6. Klicken Sie nach Abschluss der Installation des Profils auf Fertig.



7. Kehren Sie zum Browser zurück, und klicken Sie auf **Registrieren**. Notieren Sie sich die Geräte-ID, die die MAC-Adresse des Geräts enthält.



8. Klicken Sie auf Installieren, um das verifizierte Profil zu installieren.



9. Klicken Sie auf Jetzt installieren.



10. Nach Abschluss des Vorgangs bestätigt das WirelessSP-Profil, dass das Profil installiert ist. Klicken Sie auf **Fertig**.

Profile Installed Done						
and the	WirelessSP Cisco	-				
\square	Verified					
Description	ISE Profile desc	1				
Signed	ise11-mnr.corp.rf-demo.com					
Received	Mar 24, 2012					
Contains	Certificate SCEP enrollment request Wi-Fi Network					
More Details >						

11. Wechseln Sie zu **Wi-Fi Networks**, und ändern Sie das Netzwerk in **Demo1x**. Ihr Gerät ist jetzt verbunden und verwendet TLS.

Settings Wi-Fi Netw	vorks
Wi-Fi	
Choose a Network	
bibo	4 🕈 🙆
✓ Demo1x	ی ج 🔒
DemoCWA	÷ 📀
Netherstorm	4 🕈 🧕

12. Navigieren Sie auf der ISE zu **Operationen > Authentifizierungen**. Die Ereignisse zeigen den Prozess, bei dem das Gerät mit dem offenen Gastnetzwerk verbunden ist, den Registrierungsprozess mit der Komponentenbereitstellung durchläuft und nach der Registrierung der Zugriff erlaubt wird.

A Home Operations • Folicy • Administration • ee m Authentications @ Endpoint Protection Service 🕎 Alarms 👖 Reports 🔪 Troubleshoot									
Live Authentications									
🚔 Add or Remove Columns 🔹	the Ref	resh					Refresh Every 3 secon	ds • Show	Latest 20 records * within L
Time	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:27:57.052 AM		.0	paul	E8:06:80:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:27:21.714 AM			68:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM	1	ò			WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM	1	a	paul	E8:06:88:97:09:41	WLC	CWA	Any,Profiled:Apple-Pad	Pending	

 Navigieren Sie zu ISE > Administration > Identity Management > Groups > Endpoint Identity Groups > RegisteredDevices (ISE > Verwaltung der Identität > Gruppen > Endpunkt-Identitätsgruppen). Die MAC-Adresse wurde der Datenbank hinzugefügt.

🛕 Home Operations 🔻 Policy 💌 Administration 💌						
🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web Portal Management					
Identities Groups External Identity Sources	Identity Source Sequences Settings					
Identity Groups	Endpoint Group List > RegisteredDevices Endpoint Group * Name RegisteredDevices Description Asset Registered Endpoints Identity Group					
Endpoint Identity Groups Blacklist	Parent Group Save Reset					
GegisteredDevices	Endpoints Identity Group Endpoints					
	Add XRemove -					
	MAC Address					
	E8:06:88:97:09:41					

Eine SSID

In diesem Abschnitt wird eine einzelne SSID behandelt. Es wird beschrieben, wie eine direkte Verbindung mit einem 802.1x-WLAN hergestellt wird, wie ein AD-Benutzername/Kennwort für die PEAP-Authentifizierung bereitgestellt wird, wie ein Gastkonto bereitgestellt wird und wie die Verbindung mit TLS wiederhergestellt wird.

Gehen Sie wie folgt vor, um iOS im Szenario mit einer einzigen SSID bereitzustellen:

1. Wenn Sie dasselbe iOS-Gerät verwenden, entfernen Sie den Endpunkt aus den registrierten Geräten.

Endpoint Group List > RegisteredDevices Endpoint Group				
* Name	RegisteredDevices			
Description	Asset Registered Endpoint			
Parent Group				
Save Reset				
▼ Endpoints				
Identity Group	o Endpoints			
🕂 Add	×Remove *			
MAC Addre	Remove Selected			
E8:06:88:9	Remove All			

2. Navigieren Sie auf dem iOS-Gerät zu **Einstellungen > Allgemein > Profile**. Entfernen Sie die in diesem Beispiel installierten Profile.



3. Klicken Sie auf Entfernen, um die vorherigen Profile zu entfernen.





- 4. Stellen Sie mit dem vorhandenen (gelöschten) Gerät oder einem neuen iOS-Gerät eine direkte Verbindung mit dem 802.1x-Gerät her.
- 5. Stellen Sie eine Verbindung mit **Dot1x her**, geben Sie einen Benutzernamen und ein Kennwort ein, und klicken Sie auf **Beitreten**.

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

- 6. Wiederholen Sie die Schritte 90 und höher im Abschnitt zur <u>ISE-Konfiguration</u>, bis die entsprechenden Profile vollständig installiert sind.
- 7. Navigieren Sie zu ISE > Operations > Authentications, um den Prozess zu überwachen. Dieses Beispiel zeigt den Client, der bei der Bereitstellung direkt mit dem 802.1X-WLAN verbunden ist. Unter Verwendung von TLS wird die Verbindung getrennt und erneut mit dem gleichen WLAN verbunden.

Live Authentications									
🔆 Add or Remove Columns 🔹	😵 Ref	resh					Refresh Even	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		à	paul	E8:06:88:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

 Navigieren Sie zu WLC > Monitor > [Client MAC]. Beachten Sie im Clientdetail, dass sich der Client im Status "RUN" befindet, dass Data Switching auf "local" festgelegt ist und dass Authentication is Central. Dies gilt f
ür Clients, die eine Verbindung mit dem FlexConnect AP herstellen.

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	E8:06:68:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM		à	paul	E0:06:00:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

Benutzererlebnis - Bereitstellung von Android

Duale SSID

In diesem Abschnitt wird die duale SSID behandelt. Außerdem wird beschrieben, wie Sie eine Verbindung mit dem bereitzustellenden Gast und mit einem 802.1x-WLAN herstellen.

Der Verbindungsvorgang für das Android-Gerät ist dem für ein iOS-Gerät (Single- oder Dual-SSID) sehr ähnlich. Ein wichtiger Unterschied besteht jedoch darin, dass das Android-Gerät Zugriff auf das Internet benötigt, um auf den Google Marketplace (jetzt Google Play) zugreifen und den entsprechenden Agenten herunterladen zu können.

Führen Sie die folgenden Schritte aus, um ein Android-Gerät (wie in diesem Beispiel das Samsung Galaxy) im Dual-SSID-Szenario bereitzustellen:

1. Verwenden Sie im Android-Gerät Wi-Fi, um eine Verbindung mit **DemoCWA herzustellen**, und öffnen Sie das Gast-WLAN.



2. Akzeptieren Sie alle Zertifikate, um eine Verbindung zur ISE herzustellen.



3. Geben Sie im Gastportal einen Benutzernamen und ein Kennwort ein, um sich anzumelden.



4. Klicken Sie auf Registrieren. Das Gerät versucht, das Internet zu erreichen, um auf den

Google Marketplace zuzugreifen. Fügen Sie der Pre-Auth ACL (z. B. ACL-REDIRECT) zusätzliche Regeln im Controller hinzu, um den Zugriff auf das Internet zu ermöglichen.

Https://market.androi O	×
CISCO Identity Services Engine 1.1 Self-Provisioning Portal	peul Log Cut Abo
Device Registration This device has not been registered. To register this device, please enter the Device ID (MAC Address format normanice) either A-F or a digit 0-9) and a description (optional). Please click the "Register' button to install and run the Cisco W-FI Setup Assistant application. This application will inst certificates and configures your device to use secure will network. Clicking the "Register' button will redirect you to an where you can download the Cisco W-FI Setup Assistant application.	cheorem where n is fall all the recessary drold market place,
Device ID 98-0C-82-40-31-A3 Description	

5. Google listet Cisco Network Setup als Android-App auf. Klicken Sie auf INSTALLIEREN.



6. Melden Sie sich bei Google an, und klicken Sie auf INSTALLIEREN.



7. Klicken Sie auf OK.



8. Suchen Sie auf dem Android-Gerät die installierte Cisco SPW-App, und öffnen Sie sie.



- 9. Vergewissern Sie sich, dass Sie immer noch vom Android-Gerät aus beim Gastportal angemeldet sind.
- 10. Klicken Sie auf Start, um den Wi-Fi Setup Assistant zu starten.



11. Cisco SPW beginnt mit der Installation der Zertifikate.



12. Legen Sie bei entsprechender Aufforderung ein Kennwort für die Speicherung der Anmeldeinformationen fest.

М	y location					
ļ	Use wireless ne	tworks				
	Set password					
	Set a password for credential storage (At least 8 characters)					
	New password:					
	•••••					
s	Confirm new passwor	d:				
l						
	ОК	Cancel				

13. Der Cisco SPW gibt einen Zertifikatsnamen zurück, der den Benutzerschlüssel und das Benutzerzertifikat enthält. Klicken Sie zur Bestätigung auf **OK**.

Certificate na	ame					
Certificate name:						
paul						
Package contains One user key One user certificate						
OK Cancel						
Can	cel					

14. Cisco SPW fährt fort und fordert Sie zur Eingabe eines anderen Zertifikatsnamens auf, der das Zertifizierungsstellenzertifikat enthält. Geben Sie den Namen **iseca ein** (in diesem Beispiel), und klicken Sie dann auf **OK**, um fortzufahren.

Certificate n	ame				
Certificate name: iseca Package contains One CA certificate					
OK Cancel					
paul is installed.					
Can	cel				

15. Das Android-Gerät ist jetzt verbunden.



Geräteportal

Im Geräteportal können Benutzer zuvor registrierte Geräte auf eine Blacklist setzen, wenn ein Gerät verloren geht oder gestohlen wird. Außerdem können sich Benutzer bei Bedarf erneut anmelden.

Gehen Sie wie folgt vor, um ein Gerät auf die Blacklist zu setzen:

1. Um sich beim My Devices Portal anzumelden, öffnen Sie einen Browser, stellen eine Verbindung mit https://ise-server:8443/mydevices her (beachten Sie die Portnummer 8443), und melden Sie sich mit einem AD-Konto an.

CISCO My Devices Portal		
	Username Password	paul

2. Suchen Sie das Gerät unter Geräte-ID, und klicken Sie auf **Lost?** (Verloren), um die Blacklisting für ein Gerät zu starten.

Add a	New De	vice	To add a device, please ent (optional); then click submi	er the Device ID (MAC Address) a t to add the device.	and a description
Your De	vices	* Device ID Description	Submit		•
State	Device ID	Desc	nption	Action	
	E8:06:88:97:0	9:41		Edit Log	2 🚆

3. Wenn die ISE eine Warnmeldung ausgibt, klicken Sie auf Ja, um fortzufahren.



4. Die ISE bestätigt, dass das Gerät als verloren markiert ist.



5. Jeder Versuch, mit dem zuvor registrierten Gerät eine Verbindung zum Netzwerk herzustellen, wird jetzt blockiert, selbst wenn ein gültiges Zertifikat installiert ist. Dies ist ein Beispiel für ein Gerät auf der Blacklist, das nicht authentifiziert werden kann:

Live Authentications										
🙀 Add or Remove Columns =	😌 Rafi	resh					Refresh Ever	ry 3 seconds *	Show Latest 20 records	*
Time •	Status	Detals	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event	
Mar 25,12 12:49:07.851 AM	•	ò	paul	E0:06:00:97:09:41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 25,12 12:40:59.057 AM	•	ò	E0.06.00.97.09.41	EB-06-88-97-09-41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 25 12 12-40-54 197 AM		100	and	00000000000	WEC	Blackfet Access	Blackhet		Authentication falled	

6. Ein Administrator kann zu ISE > Administration > Identity Management > **Groups** navigieren, auf **Endpoint Identity Groups** > Blacklist klicken und sehen, dass das Gerät in die Blacklist aufgenommen wurde.

Julinown	Identity Groups	Endpoint Group *Name Blacklist Description Blacklist Identity Group Parent Group Save Reset • Endpoints Identity Group Endpoints		
	📇 Unknown	and Manuar -		

Führen Sie die folgenden Schritte aus, um ein Gerät auf der Blacklist wiederherzustellen:

1. Klicken Sie im My Devices-Portal auf für das Gerät neu starten.



2. Wenn die ISE eine Warnung ausgibt, klicken Sie auf Ja, um fortzufahren.



3. Die ISE bestätigt, dass das Gerät erfolgreich wiederhergestellt wurde. Verbinden Sie das wieder installierte Gerät mit dem Netzwerk, um zu testen, ob das Gerät nun zugelassen wird.



Referenz - Zertifikate

ISE erfordert nicht nur ein gültiges CA-Stammzertifikat, sondern auch ein gültiges Zertifikat, das von CA signiert wird.

Führen Sie die folgenden Schritte aus, um ein neues vertrauenswürdiges Zertifizierungsstellenzertifikat hinzuzufügen, zu binden und zu importieren:

1. Navigieren Sie zu ISE > Administration > System > Certificates, klicken Sie auf Local Certificates, und klicken Sie dann auf Add (Hinzufügen).



2. Wählen Sie Zertifikatsignierungsanforderung (CSR) generieren aus.



3. Geben Sie den Zertifikatantragsteller **CN=***<ISE-SERVER hostname.FQDN> ein.* Für die anderen Felder können Sie die Standardwerte oder die Werte verwenden, die für die CA-Einrichtung erforderlich sind. Klicken Sie auf **Senden**.

Local Certificates > Generate Generate Certificate	Certificate Signing Request Signing Request	
Certificate		
* Certificate Subject	CN=ise11-mnr.corp.rf-demo.cor	m
* Key Length	2048 💌]
* Digest to Sign With	SHA-256 *]
Submit Cancel		

4. Die ISE überprüft, ob der CSR generiert wurde.



5. Um auf den CSR zuzugreifen, klicken Sie auf die Vorgänge **Zertifikatsignierungsanforderungen**.



6. Wählen Sie den zuletzt erstellten CSR aus, und klicken Sie dann auf Exportieren.



7. Die ISE exportiert den CSR in eine PEM-Datei. Klicken Sie auf **Datei speichern**, und klicken Sie dann auf **OK**, um die Datei auf dem lokalen Computer zu speichern.



8. Suchen und öffnen Sie die ISE-Zertifikatsdatei mit einem Texteditor.



9. Kopieren Sie den gesamten Inhalt des Zertifikats.

BEGIN CERTIFICATE
MIICMzCCAZygAwIBAgIQT1/lPzR9C0W/lqfcJ2a4zTANBgkqhkiG9w0BAQUFADAl
MSMwIQYDVQQDExppc2UxMS1tbnIuY29ycC5yZi1k2W1vLmNvbTAeFw0xMjAzMTQw
MDIOMzFaFw0xMzAzMTQwMDIOMzFaMCUxIzAhBgNVBAMTGmlzZTExLW1uci5jb3Jw
LnJmLWR1bW8uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnXTshW3Qu
BcvWrtGhB2pTJ19hHVOI607XH6AM1zrbYB/0b5wDW+QFixpgE+tLSn2gOKiieGJT
yGRvymY1HSBIz8QrW1+jBQPKxQ9ossvG98w7s/WQwnP7dKI0oK6kslTNRJZBnG48
U6GquDq/5V2+LmAVQyQfhluRdFD9PUkNTwIDAQABo2QwYjAMBgNVHRMEBTADAQH/
MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBccwF10GK0YwaGQB10qS0wEwYD
VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEB
${\tt BQUAA4GBAKS+tyTC2iNKcXIygxHTWjepfDqWdoS2wFpYnGIwzoTzecGFRzfraZDi}$
1/t65UI0KQAyBRUp21TpHf+o27eDTVwW83bCmbDln0PpwhoKBMP7N8t+9uKuVcP1
osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pMhPP2hbyekAIC
END CERTIFICATE
& cut
Сору

10. Stellen Sie eine Verbindung zum Zertifizierungsstellenserver her, und melden Sie sich mit einem Administratorkonto an. Der Server ist eine Microsoft 2008-Zertifizierungsstelle unter https://10.10.10.10/certsrv (in diesem Beispiel).


11. Klicken Sie auf Zertifikat anfordern.



12. Klicken Sie auf advanced certificate request (erweiterte Zertifikatsanforderung).



13. Klicken Sie auf die zweite Option, um eine Zertifikatsanforderung mithilfe eines Base-64kodierten CMC zu senden oder



14. Fügen Sie den Inhalt aus der ISE-Zertifikatsdatei (.pem) in das Feld Gespeicherte Anforderung ein, stellen Sie sicher, dass es sich bei der Zertifikatvorlage um **Webserver** handelt, und klicken Sie auf Senden.

Microsoft Certific	ate Services labsrv.corp.rf-demo.com			
Submit a Certificate Request or Renewal Request				
To submit a sav Saved Request	red request to the CA, paste a base-64-encoded CN box.			
Saved Request:				
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	MAsGA1UdDwQEAwICrDAdBgNVHQ4EFgQUBJa5qgBc VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEB BQUAA4GBAKS+tyTCZiNKcXIygxHTWjepfDqWdoSZ 1/t65UIOKQAyBRUp21TpHf+o27eDTVwW83bCmbD1 osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM END CERTIFICATE			
Certificate Temp	late:			
	Web Server			
Additional Attribu	ites;			
Attributes:				
	Submit >			

15. Klicken Sie auf Zertifikat herunterladen.



16. Speichern Sie die Datei certnew.cer. Sie wird später verwendet, um eine Bindung mit der ISE herzustellen.

Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10? Open Save

17. Navigieren Sie von ISE-Zertifikaten zu Lokale Zertifikate, und klicken Sie auf Hinzufügen > Zertifizierungsstellenzertifikat binden.

🛕 Home Operations 🔻 Policy 🔻 Admini	stration 🔻
🔆 System 🦉 Identity Management 🔛	Network Resources 🛛 🛃 Web Portal Management
Deployment Licensing Certificates Loggin	ig Maintenance Admin Access Settings
Certificate Operations	Local Certificates
Certificate Signing Requests Certificate Authority Certificates	Edit -Add Secont XDelete Friend Import Local Server Certificate
SCEP CA Profiles OCSP Services	Generate Self-Signed Certificate Generate Certificate Signing Request Bind CA Certificate

18. Navigieren Sie zu dem Zertifikat, das im vorherigen Schritt auf dem lokalen Computer gespeichert wurde, aktivieren Sie das EAP- und das Management Interface-Protokoll (Kontrollkästchen sind aktiviert), und klicken Sie auf Senden. Der Neustart der Services bei der ISE kann einige Minuten oder länger dauern.

Certificate Operations	Bind CA Signed Certificate	
Certificate Signing Requests	Certificate	
Certificate Authority Certificates	* Certificate File C:\Users\Paul Nguyen\Downloads\certnew(4).cer	Browse_
SCEP CA Profiles	Friendly Name	
OCSP Services		
	Enable Validation of Certificate Extensions (accept only valid certificate) Protocol EAP: Use certificate for EAP protocols that use SSL/TLS tunneling Management Interface: Use certificate to authenticate the web server (GU	t)
	Override Policy Replace Certificate A certificate being imported may be determined to already exists certificate. In such a case, selection of the "Replace Certificate selections for the certificate. Storight Cancel	ist in the sy e" option w

19. Kehren Sie zur Startseite der Zertifizierungsstelle (https://CA/certsrv/) zurück, und klicken Sie auf Zertifizierungsstellenzertifikat, Zertifikatskette oder Zertifikatsperrliste herunterladen.



20. Klicken Sie auf Zertifizierungsstellenzertifikat herunterladen.

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]
© DER © Base 64
Download CA certificate

21. Speichern Sie die Datei auf dem lokalen Computer.

Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10?	Open	Save	Ŀ	ļ
			_	_

22. Wenn der ISE-Server online ist, gehen Sie zu **Zertifikate**, und klicken Sie auf **Zertifikate der Zertifizierungsstelle**.



23. Klicken Sie auf Importieren.



24. Suchen Sie nach dem Zertifizierungsstellenzertifikat, aktivieren Sie Vertrauenswürdigkeit für Clientauthentifizierung (Kontrollkästchen ist aktiviert), und klicken Sie auf Senden.

Certificate Authority Certificates > In Import a new Trusted C	aport CA (Certificate Authority) Certificate
* Certificate File Friendly Name	C:\Users\Paul Nguyen\Downloads\certnew.c Browse_
All Certificate Authority Cert authentication below: Trust for client authenti	ificates are available for selection as the Root CA for secure LDAJ
Enable Validation of	Certificate Extensions (accept only valid certificate)
Description	

25. Bestätigen Sie, dass das neue vertrauenswürdige Zertifizierungsstellenzertifikat hinzugefügt wird.

🔆 System 🦉 Identity Management	Network Resources			🛃 Web Portal Managemer		
Deployment Licensing Certificates	Logging	Mainte	nance	Admin Access	Settings	
Certificate Operations		tificat	e Autho	rity Certifica	tes	
Local Certificates Certificate Signing Requests	_ /	Edit	-Import	Export	XDelete	
Sectificate Authority Certificates		Friend	dly Name			
SCEP CA Profiles		corp-RFDEMO-CA#corp-RFDEMO-CA#00002				
🔅 OCSP Services		ise11-mnr.corp.rf-demo.com#ise11-m				

Zugehörige Informationen

- <u>Cisco Identity Services Engine Hardware Installation Guide, Version 1.0.4</u>
- <u>Cisco Wireless LAN Controller der Serie 2000</u>
- <u>Cisco Wireless LAN Controller der Serie 4400</u>
- <u>Cisco Aironet der Serie 3500</u>
- Bereitstellungsleitfaden für Flex 7500 Wireless Branch Controller
- Bring Your Own Device Einheitliche Geräteauthentifizierung und konsistenter Zugriff
- <u>Wireless BYOD mit Identity Services Engine</u>
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.