# FlexConnect 向けワイヤレス BYOD 導入ガイド

## 内容

概要 前提条件 要件 使用するコンポーネント トポロジ デバイスの登録とサプリカントのプロビジョニング 資産登録ポータル 自己登録ポータル 認証とプロビジョニング iOS(iPhone/iPad/iPod)のプロビジョニング Android のプロビジョニング デュアル SSID ワイヤレス BYOD 自己登録 シングル SSID ワイヤレス BYOD 自己登録 機能の設定 WLAN 設定 FlexConnect AP 設定 ISE の設定 ユーザ エクスペリエンス:iOS のプロビジョニング デュアル SSID シングル SSID ユーザ エクスペリエンス: Android のプロビジョニング デュアル SSID デバイス ポータル 参考:証明書 関連情報

#### 概要

モバイル デバイスは、徐々にコンピュータに近づいて強力になり、消費者間での人気が増してい ます。何百万ものデバイスが、ユーザのコミュニケーションとコラボレーションを可能にするた めに、高速 Wi-Fi を搭載して消費者に販売されます。消費者は、これらのモバイル デバイスがも たらす生産性の向上に慣れて、個人的経験を作業空間に持ち込もうとしています。これにより、 職場への個人所有デバイス持ち込み(BYOD)ソリューションの機能的な必要が生じています。

このドキュメントでは、BYOD ソリューションのブランチ導入について説明します。従業員は、 自分の新しい iPad を使用して企業のサービス セット識別子(SSID)に接続し、自己登録ポータ ルにリダイレクトされます。Cisco Identity Services Engine(ISE)は、ユーザを企業の Active Directory(AD)に対して認証し、組み込みの iPad MAC アドレスとユーザ名が含まれた証明書を 、dot1x 接続の方法として Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)の使用を強制するサプリカント プロファイルとともに iPad にダウンロードします。ISE で の許可ポリシーに基づいて、ユーザは dot1x を使用して接続し、適切なリソースへのアクセスを 取得します。

ソフトウェア リリース 7.2.110.0 より前までは、シスコ ワイヤレス LAN コントローラの ISE 機能は FlexConnect アクセス ポイント (AP)を介して関連付けるローカル スイッチング クライア ントをサポートしていませんでした。リリース 7.2.110.0 で導入されたこれらの ISE 機能は、ロ ーカル スイッチングと中央で認証されたクライアントのために FlexConnect AP でサポートされ るようになりました。さらに、ISE 1.1.1 と統合されたリリース 7.2.110.0 では、次のワイヤレス 用(次のものに限定されません)の BYOD ソリューション機能が提供されます。

- デバイスのプロファイリングとポスチャ
- デバイスの登録とサプリカントのプロビジョニング
- 個人用デバイスのオンボーディング(iOS または Android デバイスのプロビジョニング)

**注**:PCまたはMacワイヤレスラップトップやワークステーションなどの他のデバイスはサ ポートされていますが、このガイドには含まれていません。

#### 前提条件

#### 要件

このドキュメントに特有の要件はありません。

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst スイッチ
- Cisco ワイヤレス LAN (WLAN) コントローラ
- Cisco WLAN コントローラ(WLC) ソフトウェア リリース 7.2.110.0 以降
- FlexConnect モードの 802.11n AP
- Cisco ISE ソフトウェア リリース 1.1.1 以降
- Windows 2008 AD。認証局(CA)のインストール済み
- DHCP サーバ
- ドメイン ネーム システム (DNS) サーバ
- Network Time Protocol (NTP)
- ワイヤレス クライアント ラップトップ、スマートフォン、タブレット (Apple iOS、 Android、Windows、Mac)

注:このソフトウェアリリースに関する重要な情報については、『<u>Cisco Wireless LAN</u> <u>ControllerとLightweightアクセスポイントリリース7.2.110.0のリリースノート</u>』を参照して ください。ソフトウェアをロードしてテストする前に、Cisco.com のサイトにログインして 最新のリリース ノートを参照してください。 このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

#### トポロジ

これらの機能を正しく実装してテストするには、次の図に示すような最小限のネットワーク設定 が必要です。



このシミュレーションでは、FlexConnect AP を備えたネットワーク、ローカル DHCP、DNS、 WLC、および ISE を含むローカル サイトまたはリモート サイトが必要です。FlexConnect AP は 、複数の VLAN を使用したローカル スイッチングをテストするためにトランクに接続されていま す。

# デバイスの登録とサプリカントのプロビジョニング

dot1x 認証用にネイティブ サプリカントをプロビジョニングするには、デバイスを登録する必要 があります。正しい認証ポリシーに基づいて、ユーザはゲスト ページにリダイレクトされ、その ユーザの従業員クレデンシャルを使用して認証されます。ユーザにはデバイス登録ページが表示 され、デバイス情報を入力するよう求められます。デバイスのプロビジョニング プロセスが開始 します。オペレーティング システム(OS)がプロビジョニングでサポートされていない場合、 そのデバイスを MAC Authentication Bypass(MAB)アクセス用にマークするために、ユーザは 資産登録ポータルにリダイレクトされます。OS がサポートされている場合、登録プロセスが開 始され、dot1x 認証のためにデバイスのネイティブ サプリカントが設定されます。

# 資産登録ポータル

資産登録ポータルは、従業員が認証と登録プロセスによってエンドポイントのオンボーディング を開始できるようにする ISE プラットフォームの要素です。

管理者は、[endpoints identities] ページから資産を削除できます。それぞれの従業員は、登録した 資産の編集、削除、およびブラックリストへの登録を行うことができます。ブラックリストに登 録されたエンドポイントはブラックリスト ID グループに割り当てられ、ブラックリストに登録さ れたエンドポイントによるネットワークへのアクセスを防止するために許可ポリシーが作成され ます。

# 自己登録ポータル

中央 Web 認証(CWA)フローでは、従業員は、クレデンシャルを入力し、認証してから、登録 する特定の資産の特性の入力に進むことができるポータルにリダイレクトされます。このポータ ルは、自己プロビジョニング ポータルと呼ばれ、デバイス登録ポータルと似ています。ここでは 、従業員は MAC アドレスと、エンドポイントのわかりやすい説明を入力できます。

# 認証とプロビジョニング

従業員が自己登録ポータルを選択すると、プロビジョニング フェーズに進むために、有効な一連 の従業員クレデンシャルを指定するよう求められます。正常に認証されると、エンドポイントを エンドポイント データベースにプロビジョニングでき、エンドポイントの証明書が生成されます 。ページ上のリンクを使用して、従業員は Supplicant Pilot Wizard (SPW)をダウンロードでき ます。

**注**:BYODの最新のFlexConnect機能マトリックスを確認するには、シスコの記事「 <u>FlexConnect機能マトリックス</u>」を参照してください。

# iOS (iPhone/iPad/iPod)のプロビジョニング

EAP-TLS 設定の場合、ISE は Apple の Over-the-Air (OTA) 登録プロセスに従います。

- 正常に認証されると、評価エンジンが、サプリカント プロファイルになるクライアントのプロビジョニング ポリシーを評価します。
- サプリカント プロファイルが EAP-TLS 設定用である場合、OTA プロセスは、ISE が自己署 名を使用しているかまたは不明な CA によって署名されたかを判別します。いずれかの条件 に当てはまる場合、登録プロセスを開始する前に、ユーザは ISE または CA のいずれかの証 明書をダウンロードするよう求められます。
- その他の EAP 方法の場合、ISE は単に認証の成功時に最終プロファイルを適用します。

# Android のプロビジョニング

セキュリティ上の考慮事項により、Android エージェントは Android マーケットプレイス サイト からダウンロードする必要があり、ISE からはプロビジョニングできません。シスコでは、Cisco Android マーケットプレイス パブリッシャ アカウントを使用して、ウィザードのリリース候補バ ージョンを Android マーケットプレイスにアップロードします。 Android プロビジョニング プロセスは次のとおりです。

- 1. シスコは、ソフトウェア開発キット(SDK)を使用して、拡張子 .apk の付いた Android パ ッケージを作成します。
- 2. 次に、パッケージを Android マーケットプレイスにアップロードします。
- 3. ユーザは、適切なパラメータを使用してクライアント プロビジョニングでポリシーを設定 します。
- 4. デバイスの登録後、dot1x 認証が失敗すると、エンド ユーザはクライアント プロビジョニ ング サービスにリダイレクトされます。
- 5. プロビジョニングのポータル ページには、SPW をダウンロードできる Android マーケット プレイス ポータルにユーザをリダイレクトするためのボタンがあります。
- 6. サプリカントのプロビジョニングを実行するために Cisco SPW が起動します。 SPW によって ISE が検出され、ISE からプロファイルがダウンロードされます。SPW が EAP TLS の証明書およびキー ペアを作成します。SPW は、ISE に対して Simple Certificate Enrollment Protocol (SCEP)プロキシ要求呼び出しを行い、証明書を取得します。SPW は ワイヤレス プロファイルを適用します。プロファイルが正常に適用されると、SPW は再認 証を要求します。SPW は終了します。

# デュアル SSID ワイヤレス BYOD 自己登録

これは、デュアル SSID ワイヤレス BYOD 自己登録の場合のプロセスです。

- 1. ユーザはゲスト SSID に関連付けられます。
- 2. ユーザはブラウザを開き、ISE CWA ゲスト ポータルにリダイレクトされます。
- 3. ユーザは従業員ユーザ名とパスワードをゲスト ポータルに入力します。
- 4. ISE がユーザを認証し、ユーザは従業員でありゲストではないという事実に基づいて [Employee Device Registration] ゲスト ページにリダイレクトされます。
- 5. MAC アドレスが DeviceID の [Device Registration] ゲスト ページに事前に入力されています 。ユーザは説明を入力して(必要に応じて)アクセプタブル ユース ポリシー(AUP)を受 け入れます。
- 6. ユーザは [Accept] を選択して、SPW のダウンロードとインストールを開始します。
- 7. ユーザのデバイスのサプリカントが証明書とともにプロビジョニングされます。
- 8. CoA が発生し、デバイスが企業の SSID の(CORP)に再度関連付けられ、EAP-TLS(また はそのサプリカントに使用されている任意の認証方式)によって認証が行われます。

# シングル SSID ワイヤレス BYOD 自己登録

このシナリオには、Protected Extensible Authentication Protocol(PEAP)と EAP-TLS の両方が サポートされる、企業アクセス(CORP)のためのシングル SSID があります。ゲスト SSID は ありません。

これは、シングル SSID ワイヤレス BYOD 自己登録の場合のプロセスです。

- 1. ユーザは CORP に関連付けられます。
- 2. ユーザは PEAP 認証のために従業員ユーザ名とパスワードをサプリカントに入力します。
- 3. ISE がユーザを認証し、PEAP 方法に基づいて同意の許可ポリシーを提供し、[Employee Device Registration] ゲスト ページにリダイレクトします。

- 4. ユーザはブラウザを開き、[Employee Device Registration] ゲスト ページにリダイレクトされます。
- 5. MAC アドレスが DeviceID の [Device Registration] ゲスト ページに事前に入力されています 。ユーザは説明を入力して、AUP を受け入れます。
- 6. ユーザは [Accept] を選択して、SPW のダウンロードとインストールを開始します。
- 7. ユーザのデバイスのサプリカントが証明書とともにプロビジョニングされます。
- 8. CoA が発生し、デバイスは CORP SSID に再度関連付けられ、EAP-TLS によって認証が行われます。

# 機能の設定

0

設定を開始するには、次の手順を実行します。

1. このガイドでは、WLC バージョンは 7.2.110.0 以降でなければなりません。

cisco		is CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Monitor	Summary					
Summary Access Points Cisco CleanAir Statistics CDP Rogues	-ili-ili- cisco			Cisco 250	D Series Wireless C	Controller Model 2504
Clients	Controller Sum	mary		Re	gue Summary	8
Multicast	Management IP Address	10.10.10.5		A	tive Rogue APs	
	Software Version	7.2.104.16		A	tive Rogue Clients	
	Field Recovery Ima Version	ge 1.0.0		A	thoc Rogues	
	System Name	wic-11mnr		R	ogues on Wined Net	WORK

2. [Security] > [RADIUS] > [Authentication] に移動して、RADIUS サーバを WLC に追加します

li.ili. cisco	MONITOR	WLANS (	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEED	BACK
Security	RADIUS	Authentica	ation Serve	rs					
AAA     General     RADIUS     Authentication     Accounting     Fallback     TACACS+	Call Stat Use AES MAC De Network	tion ID Type I Key Wrap limiter	System M (Designed Hyphen Server	AC Address 1 for FLPS custome	ers and require	es a key wrap com	pliant RADIUS se	wer)	
LDAP	User	Managemen	t Index	Server Addre	ss Port	19	Sec	Admin Statu	15
MAC Filtering Disabled Clients User Login Policies	۲	2	1	10.10.10.60	1812	D	isabled	Enabled	٥

3. ISE 1.1.1 を WLC に追加します。

共有秘密を入力します。RFC 3576 のサポートを [Enabled] に設定します。

MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBAC
RADIUS	Authenti	ication Server	s > Edit					
Server In	dex		1					
Server Ad	dress		10.10.10.60					
Shared S	ecret Forma	at	ASCII :					
Shared S	ecret							
Confirm S	Shared Seco	ret						
Key Wrap	6	0	(Designed fo	or FIPS custom	ers and requires a l	key wrap complia	nt RADIU	S server)
Port Num	ber		1812					
Server St	atus		Enabled					
Support f	or RFC 357	6	Enabled					
Server Ti	meout		2 secon	ds				
Network	User		Enable					
Managem	ient		Enable					
IPSec			Enable					

4. RADIUS アカウンティング サーバと同じ ISE サーバを追加します。

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 Secr	et			
Port Number	1813			
Server Status	Ena	bled :		
Server Timeout	2	seconds		
Network User	1 E	nable		
IPSec		Enable		

5. 後で ISE ポリシーで使用される WLC 事前認証 ACL を作成します。[WLC] > [Security] > [Access Control Lists] > [FlexConnect ACLs] に移動し、新しい FlexConnect ACL(この例では、ACL-REDIRECT)を作成します。

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

6. ACL ルールでは、ISE との間のすべてのトラフィックを許可し、サプリカント プロビジョ ニング中のクライアント トラフィックを許可します。

最初のルール(シーケンス1)の場合:

[Source] を [Any] に設定します。[IP (ISE address)]/[Netmask] **255.255.255.255** を設定しま す。[Action] を [Permit] に設定します。

Access Control Lis	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 ‡		

2 番目のルール(シーケンス 2)の場合、[source IP (ISE address)/ mask 255.255.255.255] を [Any] **に設定し、[Action] を [Permit]** に設定します。

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. FlexConnect グループを作成します(この例では、Flex1)。

[FlexConnect Group] **> [WebPolicies] タブに移動します。**[WebPolicy ACL] フィールドで、 [Add] をクリックして [ACL-REDIRECT] または以前に作成した FlexConnect ACL を選択し ます。[WebPolicy Access Control Lists] フィールドが入力されていることを確認します。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACH	Saga Contiguiation Engl Logent Eat K
Wireless	FlexConnect Groups > Edit 'Flex1'	< Back Apply
Access Points     All APs     Radios	General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL mapping	VebPolicies
802.118/g/h Blobal Configuration Advanced Mesh RF Profiles	WebPolicies	
FlexConnect Groups MesConnect Accs > 802.11a/n > 802.11b/g/n > Media Stream	WebPolicy Access Control Lists ACL-REDIRECT	

8. [Apply] をクリックし、[Save Configuration] をクリックします。

#### WLAN 設定

WLAN を設定するには、次の手順を実行します。

1. オープン WLAN SSID(デュアル SSID の例の場合)を作成します。

WLAN名として**DemoCWA**を入力します(この例では)。[Status] で [Enabled] オプション を選択します。

WLANs > Edit 'Demo	CWA'
General Security	QoS Advanced
Profile Name	DemoCWA
Туре	WLAN
SSID	DemoCWA
Status	Enabled
Security Policies	MAC Filtering (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	F Enabled

2. [Security] タブ > [Layer 2] タブに移動して、次の属性を設定します。

レイヤ2セキュリティ:な**し**[MAC Filtering]:[Enabled] (ボックスがオンになっている)[Fast Transition]:[Disabled] (ボックスはオンになっていない)

LANS > E	dit 'Demo	CWA'	
General	Security	QoS	Advanced
Layer 2	Layer 3	AAA	Servers
Layer 2	Security 🤨 🚺 M/	lone AC Filterin	g² IZ
Layer 2 Fast Tran	Security 💁 🚺 M/ sition	lone AC Filterin	9 <sup>2</sup> 모

3. [AAA Servers] タブに移動し、次の属性を選択します。

0

eneral	Security	QoS Advanced
Layer 2	Layer 3	AAA Servers
Select AAA	servers belo	ow to override use of default servers on this WLAN
Radius Se	rvers	
Radius Se Radius	rvers Server Overw	rite interface Enabled
Radius Se Radius	rvers Server Overw	rite interface Enabled Authentication Servers Accounting Servers S Enabled S Enabled
Radius Se Radius Server	rvers Server Overw	rrite interface Enabled  Authentication Servers Accounting Servers  Enabled  IP:10.10.10.60, Port:1812 + IP:10.10.10.60, Port:1813
Radius Se Radius Server Server	rvers Server Overw 1	rite interface Enabled           Authentication Servers         Accounting Servers           Image: Servers         Image: Servers

認証およびアカウントサーバ:有効サーバ1:</SE IPアドレス>

4. [AAA Servers] タブからスクロールダウンします。[Authentication priority order for web-auth user] で、[RADIUS] **が認証に使用され、その他のものは使用されていないことを確認します** 

auth user		
Not Used	Order Used For Authentication	
LOCAL	> RADIUS	Up
	<	Dow

5. [Advanced] タブに移動し、次の属性を選択します。

Allow AAA Override	Enabled	
Coverage Hole Detection	P Enabled	DesCR Server C Overs
Enable Secolor Timeout	gr (1800 Session Timesut (sess)	DHCP Adde: Assignment T Remain
Aironat IE	9 Enabled	Nananament Frame Protection (NE)
Diagnostic Channel	l"Evabled	
Override Interface ACL	IPut None R IPut None R	1979 Class Profession # Collins
F2F Blocking Action	Disabled R	BTD9 Period (in beacan intervals)
Client Exclusion	["Evabled	
Maximum Allowed Clients	F	802.11.win (1 - 255) [1 802.113/g/n (1 - 255) [1
	Province	NAC
Diatio DF Tunneling 88	1 Endered	1 the

[Allow AAA Override]:EnabledNAC状態:Radius NAC

**注**:FlexConnect APが切断モードの場合、RADIUS Network Admission Control(NAC)はサポ ートされません。そのため、FlexConnect AP がスタンドアロン モードで、WLC への接続 を失う場合、すべてのクライアントは切断され、SSID はアドバタイズされなくなります。

6. [Advanced] タブでスクロールダウンして、[FlexConnect Local Switching] を [Enabled] に設 定します。

nabled

7. [Apply] をクリックし、[Save Configuration] をクリックします。



8. シングルおよびデュアル SSID のシナリオ用の 802.1X WLAN SSID(この例では、 Demo1x)を作成します。

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. [Security] タブ > [Layer 2] タブに移動して、次の属性を設定します。

レイヤ2セキュリテ**ィ : WPA+WPA2**[Fast Transition]:[Disabled] (ボックスはオンになって いない)[Authentication Key Management]:802.IX:**Enable** 

Layer 2 Layer 3 AAA Servers          Layer 2 Security       WPA+WPA2         MAC Filtering2       MAC Filtering2         Fast Transition       Image: Comparison of the DS image: Comparison of the Compariso	ieneral	Security	QoS	Advance
Layer 2 Security WPA+WPA2 MAC Filtering C Fast Transition Fast Transition Over the DS Reassociation Timeout 20 WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption AES TKIP Authentication Key Management 802.1X Enable	Layer 2	Layer 3	AAA S	ervers
MAC Filtering?	Layer 2	Security 😫 📔	WPA+WPA2	2
Fast Transition         Fast Transition         Over the DS         Over the DS         Reassociation Timeout         20         WPA+WPA2 Parameters         WPA Policy         WPA2 Policy         WPA2 Policy         WPA2 Encryption         Authentication Key Management         802.1X		м	AC Filtering	2 🗆
Reassociation Timeout 20 WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Encryption Authentication Key Management 802.1X Enable	1.032 11.01(34)	WWIII .		
Reassociation Timeout 20 WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Encryption Authentication Key Management 802.1X Enable				
WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption WPA2 Encryption Authentication Key Management 802.1X Enable	Over the D	s E		
WPA Policy WPA2 Policy WPA2 Encryption AES TKIP Authentication Key Management 802.1X Enable	Over the D Reassociati	S Timeout 2	0	
WPA2 Policy V WPA2 Encryption VAES TKIP Authentication Key Management 802.1X V Enable	Over the D Reassociati	S C ion Timeout 20	rs	
WPA2 Encryption PAES TKIP Authentication Key Management 802.1X PEnable	Over the D Reassociati WPA+WPA WPA Po	S on Timeout 20 A2 Paramete licy	rs	
802.1X Enable	Over the D Reassociati WPA+WPA WPA Po WPA2 P	S ion Timeout 20 A2 Paramete licy olicy	ह प्र	
802.1X 🔽 Enable	Over the D Reassociati WPA+WPA WPA Po WPA2 P WPA2 E	S ion Timeout 20 A2 Paramete licy olicy incryption	רא ארי ארי ארי	s Пткі
	Over the D Reassociati WPA+WPA WPA Po WPA2 P WPA2 E Authentic	S ion Timeout 20 A2 Paramete licy olicy incryption ation Key Ma	rs F F AE: magement	s Пткі
	Over the D Reassociati WPA+WPA WPA Po WPA2 P WPA2 E Authentic 802.1X CCKM	S C ion Timeout 20 A2 Paramete licy olicy incryption ation Key Ma	rs	s Гткі

10. [Advanced] タブに移動し、次の属性を選択します。

[Allow AAA Override]:EnabledNAC状態:Radius NAC

Allow AAA Override	F Enabled	84629
Coverage Hole Detection	P Enabled	DHCP Server Coverside
Inable Session Timesut	gr (Lans	THE ARE ADDRESS F. C.
inunat III	Finalised	teres and another to have a
Sagnutic Channel	C Enabled	management rrans Protection (MPP)
Iventide Interface ACL	IPv4 None R IPv6 None R	MPP Classit Protection # Contornal 18
OF Blocking Action	Disatived R	BTIN Period (in kear on intervals)
Sent Endusion	Wandhad Int	
Animan Minard	Timeout Value (secc)	802.33a/h (3 - 255) [3
Ciantia #	P	862.13b/g/n (1 - 255) [1
Ratic IP Turnaling M	C tratied	NAC
		NAC State Radius NAC -

11. [Advanced] タブでスクロールダウンして、[FlexConnect Local Switching] を [Enabled] に 設定します。

Enabled
· 7 manua

12. [Apply] をクリックし、[Save Configuration] をクリックします。



13. 新しい WLAN が両方とも作成されたことを確認します。

МО	NITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WL	.ANs								Entries 1 - 5 of !
Cur	rent Filte	Non	e [Change	Filter] [Clear	Filter]	I	Create New	• 6	0
	WLAN ID	Туре	Profile Na	me	v	VLAN SSID		Admin Status	Security Policies
C	1	10,85	85×			lên .		Disable	[wraz][aub(802.1×)]
r.	2	WLAR				1		Enabled	[wP42][Auth(P52)]
	2	WLAN	Demolx		C	emolx		Enabled	[WPA2][Auth(802.1X)]
	4	WLAN	DemoCWA		C	)emoCWA		Enabled	MAC Filtering
0	1	91,85	flex			le :		Creative	d Web-Auth

#### FlexConnect AP 設定

FlexConnect AP を設定するには、次の手順を実行します。

1. [WLC] > [Wireless] に移動して、ターゲット FlexConnect AP をクリックします。

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

2. [FlexConnect] タブをクリックします。



3. [VLAN Support] を有効にします(ボックスをチェック)。[Native VLAN ID] を設定し、 [VLAN Mappings] をクリックします。

VLAN Support	2	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Con	figured 63

4. ローカル スイッチング用に SSID の VLAN ID を設定します(この例では、21 **です)。** 

<u>W</u> LANs		WIRELESS	SECURITY	N
> Site-B-I	FlexAP > VLA	N Mapping	S	
e f	Site-B-FlexAP			
dio MAC d	e8:04:62:0a:68:80	D		
SSID			VLAN ID	
Demoix			21	
DemoCWA			21	
	e Site-B- dio MAC of SSID Demo1x DemoCWA	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 Mappings         e       Site-B-FlexAP         dio       MAC       e8:04:62:0a:68:80         SSID       Demo1x         DemoCWA       DemoCWA	WLANS       CONTROLLER       WIRELESS       SECURITY         > Site-B-FlexAP > VLAN Mappings         e       Site-B-FlexAP         dio       MAC       e8:04:62:0a:68:80         SSID       VLAN ID         Demo1x       21         DemoCWA       21

5. [Apply] をクリックし、[Save Configuration] をクリックします。

#### ISE の設定

ISE を設定するには、次の手順を実行します。

1. ISEサーバ<https://ise>にログイン*します*。

	Identity Services Engine
© 2012 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems log	are registered trademarks of Class Systems, inc. and/or its ++(b,)+.
affiliates in the U.S. and certain other countries.	CISCO

2. [Administration] > [Identity Management] > [External Identity Sources] に移動します。



3. [Active Directory] をクリックします。



4. [Connection] タブで次のようにします。

[Domain Name](この例では、corp.rf-demo.com)を追加して、[Identity Store Name] のデ フォルトを [AD1] に変更します。[Save Configuration] をクリックします。[Join] をクリック して、加入するために必要な AD 管理者アカウントのユーザ名とパスワードを指定します。 [Status] は緑色で表示されます。[Connected to:] を有効にします(チェックボックスがオン になっています)。

Connection Adv	vanced Settings	Groups	Attributes	
	* Do * Identity	omain Name o Store Name A	corp.rf-demo.com	
ne or more nodes may l onnection.	be selected for Join	or Leave oper	ations. If a node is ,	joined then a leave operation
ne or more nodes may l onnection. 약을 Join 약을 Leave 약	E selected for Join ≥ Test Connection →	i or Leave oper	ations. If a node is,	joined then a leave operation
ne or more nodes may l onnection. 옆 Join 안 Leave 안 J ISE Node	E selected for Join	ISE Node Ro	ations. If a node is	joined then a leave operation

5. 現在のドメイン ユーザを使用して AD への基本的な接続テストを実行します。

oonneedon.	
👷 Join 🛛 👷 Leave	👷 Test Connection 👻
ISE Node	Basic Test
Isen 1-mnr	
Test Connection * User Name: paul * Password:	×

6. AD への接続が正常に行われた場合、パスワードが正しいことを確認するダイアログが表示 されます。



7. [Administration] > [Identity Management] > [External Identity Sources] に移動します。

[Certificate Authentication Profile] をクリックします。新しい [Certificate Authentication Profile (CAP)] で [Add] をクリックします。

cisco Identity Services Engine	
Administration Administratio Administration Administration Administration Adm	nistration V
System 🏾 🖉 Identity Management	Network Resources 🛃 Web Portal Manage
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
<b>♦•</b>	150 death Departments
Certificate Authentication Profile	Cont grade grade at
2 Active Directory	🗆 Name 🐱
🚞 LDAP 🛞	
🚞 RADIUS Token 💿	
RSA SecurID	

8. CAPの名前として**CertAuth**(この例の場合)を入力し、[Principal Username X509 Attribute]で[Common Name] を選択し、[Submit] をクリックします。

Certificate Authentication Profiles List > New	Certificate Authentication Profile	
Certificate Authentication Pr	rofile	
* Name	CertAuth	
Description		
Principal Username X509 Attribute	Common Name	*
Perform Binary Certificate Comp	arison with Certificate retrieved fro	m LDAP or Active Directory
LDAP/AD Instance Name		
Submit Cancel		

9. 新しい CAP が追加されたことを確認します。

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	/ Edit 🖓 Add 🖓 Duplicate 🗙 Delete
Active Directory	Name
🚞 LDAP 💿	L Ceros n
RADIUS Token 💿	
E RSA SecurID 💿	

10. [Administration] > **[Identity Management] > [Identity Source Sequences]** に移動して、[Add] をクリックします。

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Adr	ministration 🔻
🔆 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Source	s Identity Source Sequences Settings
Identity Source Sequence	
/ Edit Add C 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. シーケンスに名前を付けます(この例では、TestSequence)。

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	
<ul> <li>Certificate</li> </ul>	e Based Authentication

12. [Certificate Based Authentication] までスクロールダウンします。

[Select Certificate Authentication Profile] **を有効にします(ボックスをチェック)。** [CertAuth](または前の手順で作成した別の **CAP プロファイル)を選択します。** 

<ul> <li>Certificate Based Authentication</li> </ul>		
Select Certificate Authentication Profile	CertAuth	•
<ul> <li>Authentication Search List</li> </ul>		

13. [Authentication Search List] までスクロールダウンします。

AD1 を [Available] から [Selected] に移動します。AD1 を最高の優先度に移動するには、 [Up] ボタンをクリックします。

<ul> <li>Authentication Search Li</li> </ul>	st		
A set of identity s	ources that will be accessed	in sequence until first authenti	cation succeeds
Available		Selected	
	*	Internal Users Internal Endpoints	*
	>> ~		v v

14. 保存するには [Submit] をクリックします。

<ul> <li>Advanced Search List Settings</li> <li>Select the action to be performed if a selected identity store cannot be accessed for authentication</li> </ul>
<ul> <li>Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"</li> <li>Treat as if the user was not found and proceed to the next store in the sequence</li> </ul>
Submit

15. 新しい ID ソース シーケンスが追加されたことを確認します。

CISCO Identity Services Engine		
🛕 Home Operations * Policy * Adminis	stration 🔻	
🔆 System 🛛 🖉 Identity Management 🖉 🖬	Network Resources 🚯 Web Portal Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Identity Source Sequence		
/ Edit -Add R Duplicate X Delete		
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. AD を使用して、デバイス ポータルを認証します。[ISE] > **[Administration] > Identity Management[] > [Identity Source Sequence]** に移動して、[MyDevices\_Portal\_Sequence] を 編集します。

🔆 System 🛛 🛃 Identity Management	Network Resources 🛛 🛃 Web
Identities Groups External Identity Sources	Identity Source Sequences
dentitu Source Seguence	0
dentry address acquence	
dentry source sequence	
/Edit 4Add Duplicate XDelete	
/ Edit +Add Duplicate XDelete	Description
Edit      Add      Duplicate      XDelete     Name     Guest_Portal_Sequence	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

17. [AD1] を [Selected] リストに追加し、AD1 を最高の優先度に移動するには、[Up] ボタンを クリックします。

▼ Authentication Search List	
A set of identity source	hat will be accessed in sequence until first authentication succeeds
Available	Selected
Internal Endpoints	AD1

18. [Save] をクリックします。



19. MyDevices\_Portal\_Sequence の Identity Store sequence に [AD1] が含まれていることを確認します。



20. Guest\_Portal\_Sequence で AD1 を追加するには、手順 16 ~ 19 を繰り返して、[Save] を クリックします。



21. Guest\_Portal\_Sequence に [AD1] が含まれていることを確認します。

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

22. WLC をネットワーク アクセス デバイス (WLC) に追加するには、[Administration] > [Network Resources] > [Network Devices] に移動して、[Add] をクリックします。

CISCO Identity Services Engine				
💧 Home Operations 🔻 Policy 💌 Adm	Network Resources	🛃 Web Portal M	lanagement	
Network Devices Network Device Groups E	xternal RADIUS Servers	RADIUS Server	Sequences	s
Network Devices	Network Devic	es		
	/ Edit Add	Duplicate	@Import	•
Network Devices     Default Device	Name	<ul> <li>IP/Mask</li> </ul>	Locatio	n

23. WLC の名前、IP アドレス、サブネット マスクなどを追加します。

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

24. [Authentication Settings] までスクロールダウンして、[Shared Secret] に入力します。これ は WLC RADIUS の共有秘密と一致する必要があります。

	Enable Authentication Settings		
	Protocol	RADIUS	
	<ul> <li>Shared Secret</li> </ul>	•••••	Show
	Enable KeyWrap		
	<ul> <li>Key Encryption Key</li> </ul>		Shov
	<ul> <li>Message Authenticator Code Key</li> </ul>		Show
	Key Input Format	ASCII   HEXI	ADECIMAL
SNMP Settings			
. SCA Attributes			

- 25. [Submit] をクリックします。
- 26. [ISE] > [Policy] > [Policy Elements] > [Results] に移動します。

CISCO Identity Service	es Engine
🛕 Home Operations 🔻	Policy  Administration
System Aldentity I Network Devices Network I Network Devices	<ul> <li>Authentication</li> <li>Authorization</li> <li>Profiling</li> <li>Posture</li> <li>Client Provisioning</li> <li>Security Group Access Egress Policy</li> </ul>
Network Devices	Network Device Authorization Policy Elements Dictionaries Conditions Results

27. [Results] **および [Authorization]** を展開し、[Authorization Profiles] をクリックして、新しい プロファイルのために [Add] をクリックします。

CISCO Identity Services Engine		60		13-
🛕 Home Operations 🔻 Policy 🔻	Administratio	n <b>T</b>		
Authentication S Authorization	Refile	Posture	e 🐻 Client	Provisioning
Dictionaries Conditions Results				
Results	۶I P	andard Autho	rization Prof	iles
<b>◆-</b> ≡ 1		Edit Add	L Duplicate	X Delete
Authentication		Name Macklist Acces		
Authorization		Gisco IP Phon	0 A6	
<ul> <li>Authorization Profiles</li> </ul>		ContractV12		
Slacklist_Access		DenvAccess		

28. このプロファイルに次の値を指定します。

名前:CWA

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

[Web Authentication] を有効にします(ボックスをチェック)。

Web認証:集中型**認証**ACL:**ACL-REDIRECT**(WLC事前認証ACL名と一致する必要があり ます)リダイレクト:デフ**ォルト** 

<ul> <li>Common Tasks</li> </ul>							
DACL Name							
ULAN VLAN							
Voice Domain Permissio	n						
Web Authentication	Centralized	•	ACL	ACL-REDIRECT	Redirect	Default	•

29. [Submit] をクリックして、新しい許可プロファイルが追加されたことを確認します。

Standard Authorization Pro	files
/ Edit -Add Duplicate	× Deleb
Name	
Blacklist_Access	
Cisco IP Phones	

30. [Add] をクリックして新しい許可プロファイルを作成します。



- 31. このプロファイルに次の値を指定します。
  - 名前:プロビジョ**ニング**

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

[Web Authentication] を有効にします(ボックスをチェック)。

Web認証値:サプリカントプロビ**ジョニング** 

<ul> <li>Common Tasks</li> </ul>			
DACL Name			
ULAN			
Voice Domain Permissio	n		
Veb Authentication	Centralized	Ŧ	ACL
	Centralized		
Auto Smart Port	Device Registration		
	Posture Discovery		
Filter-ID	Supplicant Provisioning	Dm	
		1	

ACL:**ACL-REDIRECT**(WLC事前認証ACL名と一致する必要があります)

Common Tasks		
DACL Name		
VLAN		
Voice Domain Permission		
Veb Authentication	Supplicant Provisioning *	ACL ACL-REDIRECT
Auto Smart Bort		

32. [Submit] をクリックして、プロビジョニング許可プロファイルが追加されたことを確認し ます。

Standard Authorization Profiles								
1	Edit -Add	Duplicate	×					
	Name							
	Blacklist_Access	5						
	CWA							
	- 4-							
$\Box$	Provision							

33. [Results] までスクロールダウンして、[Client Provisioning] を展開して [Resources] をクリ ックします。

🛕 Home Operations 🔻 Policy 🔻
Authentication 🥥 Authorization
Dictionaries Conditions Results
Results
<b>∲•</b> ≡ <sup>™</sup>
Authentication
Authorization
Profiling
Posture
Client Provisioning
Resources     Access     Security Group Access

34. [Native Supplicant Profile] を選択します。



35. プロファイルに名前を付けます(この例では、[WirelessSP])。

tive Supplicant Profi	le
* Name	WirelessSP
Description	

36. 次の値を入力してください。

[Connection Type]:**Wireless**SSID:**Demo1x**(この値はWLC 802.1x WLAN設定のものです)[Allowed Protocol]:**TLS**キーサイズ:**1024** 

Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demo1x
		Security	WPA2 Enterprise 👻
* Allowed Protocol	PEAP		¥
<ul> <li>Optional Settings</li> </ul>	TLS PEAP	ę	2
Submit Cancel			

37. [Submit] をクリックします。

38. [Save] をクリックします。

* Allowed Protocol	TLS	*
* Key Size	1024	*
Save Reset		

39. 新しいプロファイルが追加されたことを確認します。

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

40. [Policy] > [Client Provisioning] に移動します。



41. iOS デバイスのプロビジョニング ルールについて次の値を入力します。

[Rule Name(ルール名)]:iOSIDグループ:任意

	Rule Name		Identity	Groups		Operating System	is (	Other Conditions
- 🛯	IOS	If	Any	¢	and	Choose a	- and	Condition(s)
						Choose an O	)perating §	Bystem 👷 🕂

#### オペレーティングシス**テム:Mac iOS All**

Operating System Grou	ups
	Q
<b>◆•</b> ■ '≡	ŵ
Android	
Mac OSX	
Mac iOS All	
🔛 Windows All	۲

### 結果:WirelessSP(以前に作成されたネイティブサプリカントプロファイル)

ther Conditions	Results
	then Result 🕀 🥎

[Results] > [Wizard Profile] (ドロップダウン リスト) > [WirelessSP] に移動します。



WizardProfile	
	م
<b>◆-</b> ■ '≣	<u>ن</u> ي پ
Clear Selection	
Wireless	

42. iOS プロビジョニング プロファイルが追加されたことを確認します。

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

43. 最初のルールの右側で、[Actions] ドロップダウン リストを見つけて、[Duplicate below] **ま** たは [Duplicate above] を選択します。



44. 新しいルールの名前を [Android] に変更します。

		Rule Name
. 🖸	•	iOS
	•	Android

45. オペレーティング システムを [Android] に変更します。



- 46. 他の値は未変更のままにします。
- 47. [Save] (画面左下)をクリックします。



48. [ISE] > [Policy] > [Authentication] に移動します。



49. Wireless\_MAB を含めるよう条件を変更して、[Wired\_MAB] を展開します。



50. [Condition Name] ドロップダウン リストをクリックします。



51. [Dictionaries] [Compound Condition] を選択します。

Dictionaries	
	P
<b>∲•</b>	\$~
🪞 Simple Condition	۲
Compound Condition	to

52. [Wireless\_MAB] を選択します。



53. ルールの右側で、矢印を選択して展開します。

	: If [	Wireless_MAB	¢	allow protocols	Allowed Protocol : Default Netw	and	LZ_
l							

54. ドロップダウン リストから次の値を選択します。

[Identity Source]:**TestSequence**(以前に作成された値)認証に失敗した場合:**Reject**ユー ザが見つからない場合:**Continue**プロセスが失敗した場合:**Drop** 

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

55. [Dot1X] ルールにアクセスして、次の値を変更します。

1	*	Dot1X	: If	Wired_802.	1X @	- <del>2</del>	allow protocol
		Default Rule (If no match)	: a	llow protocols	Allowed	Proto	col : Default Ne

Cor	npound Condition
	م
4	· 🔳 📜 🌸
	Wired_MAB
	Wireless_MAB
	Wired_802.1X
	Wireless_802.1X dby
	Switch_Local_Web_Authentication
	WLC_Web_Authentication
: If : all	Wired_802.1X allo Add All Conditions Below t Condition Name Wireless 802.1X

条件:Wireless\_802.1X

[Identity Source]:TestSequence

Identity Source TestSequence	se for authe
Options	Identity Source List
If authentication failed Reject	
If user not found Reject	
If process failed Drop 🔹	<b>∲•</b>
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS	Internal Endpoints
it is not possible to continue processing when authentication fails a	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. [Save] をクリックします。



57. [ISE] > [Policy] > [Authorization] に移動します。



58. デフォルトのルール([ブラックリストデフォルト(Black List Default)]、[プロファイル済み (Profiled)]、[デフォルト(Default)]など)は、インストールからすでに設定されています。最 初の2つは無視できます。デフォルトのルールは後で編集されます。

st Match	ed Rule Applies 🔹		
Exceptio	ns (0)		
Standar	d		
Stat	tus Rule Name	Conditions (identity groups and other conditions)	Permissions
	Black List Default	if Blacklist	then Blacklist_Access

59. 2 番目のルール([Profiled Cisco IP Phones])の右側で、[Edit] の横にある下矢印をクリックして、[Insert New Rule Below] を選択します。



新しく [Standard Rule #] が追加されます。

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

60. ルール名を [Standard Rule #] から [OpenCWA] に変更します。このルールは、デバイスを

プロビジョニングするために、ゲスト ネットワークへの着信時にオープン WLAN(デュア ル SSID)で登録プロセスを開始します。

-	OpenCWA	
---	---------	--

61. [Condition(s)] のプラス記号([+])をクリックして、条件のプラス記号(+)をクリックして、[Existing Condition from Library] を選択します。

† Cisco-IP-Phone		then Cisco_IP_Phone
f Any $\diamondsuit$ and f no matches, then Perm	Select Condition	then AuthZ Pro

62. [Compound Conditions] [Wireless\_MAB] を選択します。

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	
Add All Conditions B	
Condition Name	
Select Condition	

63. [AuthZ Profile] でプラス記号([+])をクリックして、[Standard] を選択します。
| Icy Elements     Image: Construction of the second of the se |                | Profiles                                  |
|--|----------------|---|
| Icy Elements   |                | ٩   |
| cklist_Access<br>co_JP_Phones  | licy Elements  | <b>∲-</b> ∎ '≣ ⊗.                         |
| rmissions<br>cklist_Access<br>co_JP_Phones   |                | 🚞 Inline Posture Node 💿                   |
| rmissions<br>cklist_Access<br>co_IP_Phones   |                | 🚞 Security Group 🛞                        |
| rmissions<br>ckilst_Access<br>co_IP_Phones   |                | Standard 💦 🛞                              |
| ckilst_Access<br>co_IP_Phones  | rmissions      |   |
| co_IP_Phones   | cklist_Access  |   |
|  | co_IP_Phones   |   |
| AuthZ Profil   | AuthZ Profil 👄 |   |
| Select an item 📀 📼 🔶   | Select an item | <ul> <li>O     <li>→     </li> </li></ul> |
|  |                |   |

64. 標準の [CWA] (以前に作成した許可プロファイル)を選択します。

Standard	
	(م
🔶 - 🗐 📜	\$ <u>*</u>
-	
CWA Jha	
Circo D Phana	

65. 正しい条件と許可とともにルールが追加されたことを確認します。

Verless\_MAB 💠 then CWA 💠

66. (ルールの右側にある) [Done] をクリックします。



67. 同じルールの右側で、[Edit] の横にある下矢印をクリックして、[Insert New Rule Below] を

68. ルール名を [Standard Rule #] から [PEAPrule] **に変更します(この例の場合)。**このルー ルは PEAP 用です(シングル SSID のシナリオでも使用されます)。Transport Layer Security(TLS)なしで 802.1X を認証したかどうか、およびネットワーク サプリカントの プロビジョニングが以前に作成した「Provision」許可プロファイルを使用して開始された かどうかを確認します。

1		OpenCWA	if Wireless_MAB	then CWA
1	- [	Standard Rule 1	Any 💠 and Condition(s)	💠 then Auth2 Profil 💠

69. 条件を [Wireless\_802.1X] に変更します。

Cor	ndition(s)	then AuthZ Profil	
n 💾	Add All Conditions Below t	to Library	
	Condition Name	Expression	
440	Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	\$* <b>-</b>

70. 条件の右側にある歯車アイコンをクリックし、[Add Attribute/Value] を選択します。これは、OR 条件ではなく AND 条件です。

	<b>ģ</b> ₊	
	Add Attribute/Value	
	Add Condition from 🖉 ary	
Delete		

71. [Network Access] を見つけて選択します。

			Dictionaries	
				Q
			<b>∲-</b>	ŵ.
os and other conditions)				-
		then		
		then		
		then		
Condition(s)	0			
tAccess				
Condition Name	Expression			
Wireless_802.1X 🛇	Radius:Service-	Type E	Network Access	
¢	Select Attric	ute 🤇		

72. [AuthenticationMethod] を選択して、次の値を入力します。



#### AuthenticationMethod: Equals

Network Access:Au🛇	<b>•</b>
	Equals Not Equals

[MSCHAPV2] を選択します。

S Framed AND Radius:NAS-Port			
Equals •	<b>•</b>		
	CHAP/MD5		
	Lookup		
	MSCHAPV1		
	MSCHAPV2		
	PAP_ASCII		
	x509_PKI		

これはルールの例です。条件がANDであることを確認してください。

and	Condition(s)	🗢 then 🛛 AuthZ Profil 💠		
	Condition Name	Expression	AND	
	Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port		<b>ŵ</b> ∙
	♦	Network Access:Au Equals * MSCHAPV2 *	0	ŵ <b>.</b>

73. [AuthZ Profile] で、[Standard] > [Provision](以前に作成した許可プロファイル)を選択し ます。

then	AuthZ Profil	Done
	Select an item 📀	-+

Standard	ž _
	و م
<b>∲-</b> ■ 1	ŵ
Provision	
2)	

74. [Done] をクリックします。



75. PEAPrule の右側で、[Edit] の横にある下矢印をクリックして、[Insert New Rule Below] を 選択します。



76. ルール名を [Standard Rule #] から [AllowRule] **に変更します(この例の場合)。**このルー ルは、証明書がインストールされた登録済みデバイスへのアクセスを許可するために使用 されます。

l	2 Plan Street and Dates	1	Any /	1	Condition(#)		there	Auth-7 Deedl	~
I			Mill	-	Condition(s)	~		Adding Province	~

77. [Condition(s)] で [Compound Conditions] を選択します。

0	Dictionaries	
		P
	<b>₫•</b>	\@+
ant Dravisioning	Simple Conditions	۲
	Compound Conditions	R.
	Time and Date Conditions	82
Condition(s)		
Add All Conditions B		
Condition Name		

78. [Wireless\_802.1X] を選択します。



79. AND 属性を追加します。

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

80. 条件の右側にある歯車アイコンをクリックし、[Add Attribute/Value] を選択します。



81. [Radius] を見つけて選択します。

6			Dictionaries	
	La		<b>•</b> •	
Client Provisioning 🛛 🚊 Securi	ity Group Access		🚞 diter	
			Caco-dettre	
		then	Cause in Pacification	
		then	aesace 🗧	
		then	🛄 EndPointe	
an and second shares and	the of		🔛 Guest	
etwork access: Authenticationme	thod	then	🛄 Allenthylining	
Wireless 802.1X Network Acce	ss:A 🗢		🚞 Internal.teer	
<b></b>			Alcosoft 🔛	
Condition Name	Expression		Entropy Access	AND V
			🧰 Radius	
Wireless_802.1X 📀	Radius:Service	Type E	Sectors 1	20-
٥	Select Attri	bute 🤇		o

82. [Calling-Station-ID--[31]] を選択します。



83. [Equals] を選択します。

Radius:Service-Type EQUALS Fr	amed AND Radius:NAS	3-Port
Radius:Calling-Statio	<b>T</b>	<b>O</b>
No	it Equals	

84. [CERTIFICATE] に移動して、右矢印をクリックします。

Standard
<b>⇔</b> • ■ 1
Carthader, Access
CHA
😋 Caco JP JPares
Carebrast9122
Carty-Access
Ca Discovery
Carloyee/11
PermitAccess
😋 Provision 🕤

85. [Subject Alternative Name] を選択します。



86. [AuthZ Profile] で [Standard] を選択します。

	Profiles	
		۵.
	<b>◆-</b> ■ '≡	\$\$ <b>~</b> _
cy Elements	🔚 Jake Posture Rode	
	🛄 fiscarly Group	
	Standard	J.
o_IP_Phones		
A.		E
vision	-	E
AuthZ Profil		
Select an item	1	

87. [Permit Access] を選択します。



88. [Done] をクリックします。



これはルールの例です。

I	OpenCHA /	Webs Jild	there is a	Сня
1	Riha i	Medico, 802.5X <==: Network Access AuthenticationRethod 822.96.5 R8CH48742 3		Provision
1	AllowRule	Wireless_802:1X Radus:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name		PermitAccess

89. [Default] ルールを見つけて、[PermitAccess] を [Deny Access] に変更します。

Default	if no matches, then	PermitAccess

90. [Default] ルールを編集するには、[Edit] をクリックします。



91. PermitAccess の既存の AuthZ プロファイルに移動します。



92. [Standard] を選択します。



93. [DenyAccess] を選択します。

Sta	ndard
\$	· 🗐 🗉 📄
å	Cerk Cerk
8	Cano, JP JPhones ContractV12
0	DenyAccess

94. 一致が見つからない場合は、[Default] ルールに [DenyAccess] が指定されていることを確認 します。

1	Default	if no matches, then	DenyAccess	÷

95. [Done] をクリックします。



次に、このテストに必要な主なルールの例を示します。これらはシングルSSIDまたはデュ アルSSIDのシナリオに適用できます。

OpenCWA	Wireless_MAB	then CWA
PEAPrule	(Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 )	then Provision
AllowRule	(Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name )	then PermitAccess
Default	no matches, then DenyAccess	

96. [Save] をクリックします。



97. [ISE] > [Administration] > [System] > [Certificates] に移動して、SCEP プロファイルで ISE サーバを設定します。



98. [Certificate Operations] で [SCEP CA Profiles] をクリックします。



99. [Add] をクリックします。

/ Edit -Add XDelete	
Name	

100. このプロファイルについて次の値を入力します。

名前:**mySCEP**(この例では)URL:**https://**<ca-server>**/CertSrv/mscep/**(CAサーバの設 定で正しいアドレスを確認します)

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

101. SCEP 接続をテストするには、[Test Connectivity] をクリックします。



102. この応答は、サーバ接続が正常であることを示しています。



103. [Submit] をクリックします。



104. サーバ応答により、CA プロファイルが正常に作成されたことが示されます。



105. SCEP CA プロファイルが追加されたことを確認します。

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

# ユーザ エクスペリエンス:iOS のプロビジョニング

#### デュアル SSID

このセクションでは、デュアル SSID について扱われ、ビジョニングするゲストへの接続方法と 802.1x WLAN への接続方法が説明されます。

デュアル SSID のシナリオで iOS をプロビジョニングするには、次の手順を実行します。

1. iOS デバイスで、[Wi-Fi Networks] に移動して、[DemoCWA](WLC で設定済みのオープン WLAN)を選択します。

Settings Wi-Fi Networ	ks
Wi-Fi	
Choose a Network	
bibo	47 🧕
Demo1x	۵ ج 🗈
✓ DemoCWA	<b>२ 0</b>
Netherstorm	4 🕈 🙆
Other	>
Ask to Join Networks	ON
Known networks will b	e joined

2. iOS デバイスで Safari ブラウザを開き、到達可能な URL(たとえば、内部または外部 Web サーバ)にアクセスします。ISE がポータルにリダイレクトされます。[Continue] をクリッ クします。

Web Authentication Redirect
se11-mnr.corp.rf-demo X Google
Cannot Verify Server Identity
Safari cannot verify the identity of "ise11-mnr.corp.rf-demo.com". Would you like to continue anyway?
Cancel
Details
Continue

3. ログインのためにゲスト ポータルにリダイレクトされます。



4. AD ユーザ アカウントとパスワードを使用してログインします。プロンプトが表示されたら CA プロファイルをインストールします。



5. CA サーバの信頼できる証明書の [Install] をクリックします。



6. プロファイルが完全にインストールされたら [Done] をクリックします。



7. ブラウザに戻って、[Register].をクリックします。デバイスの MAC アドレスが含まれてい るデバイス ID をメモします。



8. 確認したプロファイルをインストールするには、[Install] をクリックします。



9. [Install Now] をクリックします。



10. プロセスの完了後に、WirelessSP プロファイルがインストールされたことを確認します。 [Done] をクリックします。

Profile Installed Done							
X X	WirelessSP Cisco						
	<b>Verified</b>						
Description ISE Profile desc							
Signed	ise11-mnr.corp.rf-demo.com	I					
Received	Mar 24, 2012	I					
Contains	Certificate SCEP enrollment request Wi-Fi Network						
More Details >							

11. [Wi-Fi Networks] に移動して、ネットワークを [Demo1x] に変更します。これで、TLS を使用してデバイスが接続されます。

Settings Wi-Fi Netwo	orks
Wi-Fi	
Choose a Network	
bibo	4 🗢 🧕
✓ Demo1x	و ج 🔒
DemoCWA	÷ 📀
Netherstorm	470

12. ISE で、[Operations] > **[Authentications]** に移動します。イベントに、デバイスがオープン なゲスト ネットワークに接続されるプロセスが表示され、サプリカント プロビジョニング を使用して登録プロセスが行われて、登録後にアクセスが許可されます。

A Home Operations	• Fol	cy 🔹	Administration •	Alarris 🦵 Report	ts 🔪 Trouble	shoot			100
Live Authentications									
Add or Remove Columns •	the Ref	resh					Refresh Every 3 second	nds • Show	Latest 20 records • within L
Time	Status	Detals	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			68:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM	1				WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM		a	paul	E8:06:89:97:09:41	WLC	CWA	Any,Profiled:Apple-Pad	Pending	

13. [ISE] > [Administration] > [Identity Management] > [Groups] > [Endpoint Identity Groups] >

[RegisteredDevices] に移動します。MAC アドレスがデータベースに追加されます。

System Aldentity Management Network Resources Identities Groups External Identity Sources Identity Source Seq. Identity Groups Identity	Web Portal Management ences Settings isteredDevices isteredDevices t Registered Endpoints Identity Group
Identities       Groups       External Identity Sources       Identity Source Sequence         Identity Groups       Endpoint Group List > Reg         Identity Groups       Image: Sequence       Image: Sequence         Image: Sequence       Image: Sequence       Image: Sequence       Image: Sequence         Image: Sequence       Image: Sequence       Image: Sequence       Image: Sequence         Image: Sequence       Image: Sequence       Image: Sequence       Image: Sequence         Image: Sequence       Image: Sequence       Image: Sequence       Image: Sequence	ences Settings isteredDevices isteredDevices it Registered Endpoints Identity Group
<ul> <li>Profiled</li> <li>RegisteredDevices</li> <li>Unknown</li> <li>Endpoints</li> <li>Identity Group End</li> <li>Add</li> <li>MAC Address</li> <li>E8:06:88:97:0</li> </ul>	coints Remove • 0:41

### シングル SSID

これはシングル SSID に関するセクションであり、802.1x WLAN に直接接続する方法、PEAP を 使用して認証するための AD ユーザ名/パスワードを指定する方法、およびゲストを介したプロビ ジョニングと TLS との再接続を行う方法について説明されています。

シングル SSID のシナリオで iOS をプロビジョニングするには、次の手順を実行します。

1. 同じ iOS デバイスを使用する場合、登録済みデバイスからエンドポイントを削除します。

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

2. iOS デバイスで、[Settings] > **[Generals]** > **[Profiles]** に移動します。この例でインストールさ れたプロファイルを削除します。



3. 前のプロファイルを削除するには、[Remove] をクリックします。





- 4. 既存の(クリアされた)デバイスを使用するか、新しい iOS デバイスを使用する場合は 802.1x に直接接続します。
- 5. Dot1x に接続して、[Username] と [Password] に入力して、[Join] をクリックします。

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

- 6. 適切なプロファイルが完全にインストールされるまで、「<u>ISE の設定」セクションのステップ 90 以降を繰り返します。</u>
- 7. プロセスをモニタするには、[ISE] > [Operations] > [Authentications] に移動します。 は、802.1X WLAN に直接接続されたクライアントがプロビジョニングされ、切断されてか ら、TLS を使用して同じ WLAN に再接続する例を示します。

Live Authentications									
😳 Add or Ramove Columns 👻 🏀 Refresh Refresh Prov 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	2	o	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

8. [WLC] > [Monitor] > [Client MAC] に移動します。クライアントの詳細から、クライアントが RUN 状態になっていて、その [Data Switching] は [local] に設定され、[Authentication] が [Central] になっていることがわかります。これは、FlexConnect AP に接続されているクラ イアントに当てはまります。

Live Authentications									
🚔 Add or Remove Columns	- 😸 Ra	fresh					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 A	н 🗹	ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 A	н 🛃	ò	E8:05:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 A	N 🛃	à	piul	E8-06-88-97-09-41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

ユーザ エクスペリエンス:Android のプロビジョニング

## デュアル SSID

このデュアル SSID に関するセクションでは、プロビジョニングするゲストへの接続方法と 802.1x WLAN への接続方法を説明します。

Android デバイスへの接続プロセスは、iOS デバイス(シングルまたはデュアル SSID)への接続 プロセスと非常によく似ています。違いは、Android デバイスでは、Google マーケットプレイス (現在では Google Play)にアクセスし、サプリカント エージェントをダウンロードするには、 インターネットへのアクセスが必要であるという点です。

デュアル SSID のシナリオで Android デバイス(この例で Samsung Galaxy など)をプロビジョ ニングするには、次の手順を実行します。

1. Android デバイスで、Wi-Fi 経由で [DemoCWA] に接続して、ゲスト WLAN を開きます。



2. ISE に接続するには、証明書を受け入れます。



3. ログインするには、ゲスト ポータルで [Username] と [Password] に入力します。



4. [Register] をクリックします。デバイスは Google マーケットプレイスにアクセスするため にインターネットに到達しようとします。インターネットへのアクセスを許可するには、コ ントローラで追加のルールを事前認証 ACL(ACL-REDIRECT など)に追加します。

🕝 https://market.androi 🔾	×
CISCO Identity Services Engine 1.1 Self-Provisioning Portal	paul Log Out Abo
Device Registration This device has not been registered. To register this device, please enter the Device ID (MAC Address format normannel) either A-F or a digt 0-19 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.	conconcos where n is tall all the necessary droid market place,
Device 10 98-0C-82-40-31-A9 Description	

5. Google には [Android App] に [Cisco Network Setup] がリストされます。[INSTALL] をクリ ックします。



6. Google にサインインして、[INSTALL] をクリックします。



7. [OK] をクリックします。



8. Android デバイスで、インストールされた Cisco SPW アプリを見つけて開きます。



- 9. Android デバイスからまだゲスト ポータルにログインしたままにしてください。
- 10. Wi-Fi Setup Assistant を開始するには、[Start] をクリックします。



11. Cisco SPW が証明書のインストールを開始します。



12. プロンプトが表示されたら、クレデンシャルを保存するためのパスワードを設定します。



13. ユーザ キーと証明書が含まれている証明書名が示された Cisco SPW に戻ります。[OK] を クリックして確認します。

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

14. Cisco SPW はプロセスを続行して、CA 証明書が含まれている別の証明書名のプロンプト を表示します。名前(この例では **iseca)を入力し、[OK]** をクリックして続行します。

15. Android デバイスが接続されます。



# デバイス ポータル

My Devices ポータルでは、ユーザは、デバイスの損失/盗難の場合に以前に登録したデバイスを ブラックリストに登録できます。また、ユーザは必要に応じて再度リストに入れることもできま す。

デバイスをブラックリストに登録するには、次の手順を実行します。

1. My Devices ポータルにログインするには、ブラウザを開き、https://iseserver:8443/mydevices(ポート番号は 8443 であることに注意してください)に接続して、 AD アカウントを使用してログインします。

CISCO My Devices Portal		
	Username Password	paul

2. [Device ID] でデバイスを見つけて、[Lost?] をクリックしてデバイスのブラックリストへの 登録を開始します。

Add a New Device	To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.	
* Device ID Description	Submit	<del>0</del>
State Device ID Des	scription Action	
E8:06:88:97:09:41	Edit   Logi?   🗐	

3. ISE が警告を表示したら、[Yes] をクリックして続行します。



4. ISE は、デバイスを [lost] として正常にマークしたことを確認します。



5. 以前に登録されたデバイスを使用してネットワークに接続しようとすると、有効な証明書が インストールされている場合でもブロックされます。次に、認証に失敗する、ブラックリス トに登録されたデバイスの例を示します。

Live Authentications										
🙀 Add or Remove Columns = 🏀 Refresh Refresh Every 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	E8:06:08:97:09:41	EB-06-88-97:09-41	WLC	Blacklist_Access	Blacklet		Authentication falled	
Mar 25 12 12-40-54 127 AM			and	100000000000	WEC	Blackfet Access	Blacklet		Authentication field	

6. 管理者は、[ISE] > [Administration] > [Identity Management] > [Groups] に移動し、[Endpoint Identity Groups] > [Blacklist] をクリックして、ブラックリストに登録されたデバイスを確認

#### できます。

رم .	and a start of the		
	Allow Distant		
Image: Second	Description Blackist Identity Group		
Enclose service aroups     Blackist     Profiled	Save Reset		
RegisteredDevices	Identity Group Endpoints		
	Add KRemove -		
	MAC Address		
	Add MAC Addres		

ブラックリストに登録したデバイスを復元するには、次の手順を実行します。

1. My Devices ポータルから、そのデバイスの [Reinstate] をクリックします。



2. ISE が警告を表示したら、続行するには [Yes] をクリックします。



3. ISE は、デバイスが正常に復元されたことを確認します。復元したデバイスをネットワーク に接続して、デバイスが許可されていることをテストできます。



## 参考:証明書

ISE では、有効な CA ルート証明書のみでなく、CA によって署名された有効な証明書が必要です。

新しい信頼できる CA 証明書を追加、バインド、およびインポートするには、次の手順を実行し ます。

1. [ISE] > **[Administration] > [System] > [Certificates]** に移動し、[Local Certificates] をクリック して、[Add] をクリックします。



2. [Generate Certificate Signing Request] (CSR)を選択します。

Loc	al Cer	tificates	6	
1	Edit	Add	Export	XDelete
	Friend Defau	Import L Generati Generati Bind CA	ocal Server C e Self-Signed e Certificate S Certificate	ertificate Certificate Signing Request

3. [Certificate Subject] に [CN=<ISE-SERVER hostname.FQDN>] を入力します。他のフィール ドには、デフォルトまたは CA の設定で必要な値を使用できます。[Submit] をクリックしま す。

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 は、CSR が生成されたことを確認します。



5. CSR にアクセスするには、[Certificate Signing Requests] 操作をクリックします。



6. 新しく作成した CSR を選択して、[Export].をクリックします。



7. ISE は CSR を .pem ファイルにエクスポートします。[Save File] をクリックして、[OK] を クリックし、ファイルをローカル マシンに保存します。



8. ISE 証明書ファイルを見つけて、テキスト エディタで開きます。



9. 証明書の内容全体をコピーします。



10. CA サーバに接続して、管理者アカウントを使用してログインします。サーバは、 https://10.10.10.10/certsrv の Microsoft 2008 CA です(この例の場合)。

<b>G</b> • <b>M</b>	ktps://10.10.10.10/certsrv/	eo 🤤 💌 🤇
Windows Securit	y	×
Connecting to 10	0.10.10.10.	
	administrator	
-		
	Domain: KFT7 Remember my credentials	
	ОК	Cancel

11. [Request a certificate] をクリックします。



12. [advanced certificate request] をクリックします。



13. 2番目のオプションをクリックして、Submit a certificate request by using a base-64encoded CMC or ....



14. ISE 証明書ファイル(.pem)の内容を [Saved Request] フィールドに貼り付けて、 [Certificate Template] が [Web Server] であることを確認し、[Submit] をクリックします。

Microsoft Certific	ate Services labsrv.corp.rf-demo.com
Submit a Certi	ficate 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/t65UIOKQAyBRUp21TpHf+o27eDTVwW83bCmbD1 osMN8EmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pH END CERTIFICATE
Certificate Temp	late:
	Web Server
Additional Attribution	ites:
Attributes:	
	Submit >

15. [Download certificate] をクリックします。



16. certnew.cerファイルを保存します。このファイルは、後でISEとのバインドに使用されます。



17. ISE の [Certificates] から、[Local Certificates] に移動し、[Add] > [Bind CA Certificate] をク リックします。
| 🛕 Home Operations 🔻 Policy 💌 Ad  | ministration 🔻                                |
|--|---|
| 🔆 System 🛛 👰 Identity Management   | 🖬 Network Resources 🛛 🛃 Web Portal Management |
| Deployment Licensing Certificates Lo   | igging Maintenance Admin Access Settings      |
| Certificate Operations Certificate Operations Certificate Signing Requests Certificate Authority Certificates SCEP CA Profiles CCSP Services | Local Certificates                            |

18. 前の手順でローカル マシンに保存した証明書を参照して、[EAP] **と [Management** Interface] の両方のプロトコルを有効にします(ボックスをチェック)。その後、 [Submit].をクリックします。ISE がサービスを再起動するのに数分以上かかる場合があり ます。

Certificate Operations	Local Certificates > Bind CA Signed Certificate Bind CA Signed Certificate Certificate	
Certificate Authority Certificates     SCEP CA Profiles	Certificate File C:\Users\Paul Nguyen\Downloads\certnew(4).cer     Browse_ Friendly Name	
	Enable Validation of Certificate Extensions (accept only valid certificate)	
	Override Policy  Replace Certificate A certificate being imported may be determined to already exist in the sys certificate Selections for the certificate.  Cancel	

19. CA のランディング ページ(https://CA/certsrv/)に戻り、[Download a CA certificate, certificate chain, or CRL] をクリックします。



20. [Download CA certificate] をクリックします。

Microsoft Active Directory Certificate Services - cor			
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			
Downkoad latest delta CRL			

21. [Save] をクリックして、ファイルをローカル マシンに保存します。



22. ISE サーバがオンラインの状態で、[Certificates] に移動して、[Certificate Authority Certificates] をクリックします。



23. [Import] をクリックします。



24. CA 証明書を参照して、[Trust for client authentication] **を有効にし(ボックスをチェック** )、[Submit] をクリックします。

Certificate Authority Certificates > In Import a new Trusted C	<sup>nport</sup> 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. 信頼できる新しい CA 証明書が追加されたことを確認します。

😽 System 🛛 👰 Identity Management	Network Resources	🛃 Web Portal Managemer	
Deployment Licensing Certificates	Logging Maintenance	Admin Access Settings	
Certificate Operations	Certificate Auth	Certificate Authority Certificates	
Certificate Signing Requests	/ Edit 🕂 Imp	ort Delete	
Sertificate Authority Certificates	Friendly Name      corp-RFDEMO-CA#corp-RFDEMO-CA#00002      ise11-mnr.corp.rf-demo.com#ise11-mnr.corp		
🜞 SCEP CA Profiles			
🔅 OCSP Services			

## 関連情報

- Cisco Identity Services Engine のハードウェア インストール ガイド、リリース 1.0.4
- <u>Cisco 2000 シリーズ ワイアレス LAN コントローラ</u>
- <u>Cisco 4400 シリーズ ワイアレス LAN コントローラ</u>
- <u>Cisco Aironet 3500 シリーズ</u>
- Flex 7500 ワイヤレス ブランチ コントローラ導入ガイド
- アイデンティティ サービス エンジンのワイヤレス BYOD
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。