FreeRadius と WLC 8.3 を使用した 802.1x -PEAP の設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 設定 <u>ネットワーク図</u> httpd サーバと MariaDB のインストール CentOS 7 への PHP 7 のインストール FreeRADIUS のインストール FreeRADIUS FreeRADIUSでの認証、許可、アカウンティング(AAA)クライアントとしてのWLC WLC上のRADIUSサーバとしてのFreeRADIUS **WLAN** freeRADIUS データベースへのユーザの追加 freeRADIUS の証明書 エンド デバイスの設定 FreeRADIUS証明書のインポート WLANプロファイルの作成 確認 WCL での認証プロセス トラブルシュート

概要

このドキュメントでは、802.1xセキュリティとProtected Extensible Authentication Protocol(PEAP)をExtensible Authentication Protocol(EAP)として使用するワイヤレスローカルエ リアネットワーク(WLAN)をセットアップする方法について説明します。 FreeRADIUS は外部 Remote Authentication Dial-In User Service(RADIUS)サーバとして使用されます。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- Linux
- Vimエディタ
- AireOSワイヤレスLANコントローラ(WLC)

注:このドキュメントは、PEAP-MS-CHAPv2認証にfreeRADIUSサーバで必要な設定の例 を読者に示すことを目的としています。このドキュメントに記載されている freeRADIUS サ ーバの設定は、ラボでテスト済みであり、予期されているとおりに機能することが判明して います。Cisco Technical Assistance Center(TAC)は freeRADIUS サーバ設定をサポート していません。

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。

- CentOS7またはRed Hat Enterprise Linux 7(RHEL7)(推奨1 GB RAMおよび20 GB HDD)
- WLC 5508 v8.3
- MariaDB (MySQL)
- FreeRADIUS
- PHP 7

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。

設定

ネットワーク図



httpd サーバと MariaDB のインストール

ステップ1:次のコマンドを実行して httpd サーバと MariaDB をインストールします。

[root@tac-mxwireless ~]# yum -y update [root@tac-mxwireless ~]# yum -y groupinstall "Development Tools" [root@tac-mxwireless ~]# yum -y install httpd httpd-devel mariadb-server mariadb ステップ 2: httpd (Apache)と MariaDB サーバを起動し、有効にします。

[root@tac-mxwireless ~]# systemctl enable httpd [root@tac-mxwireless ~]# systemctl start httpd [root@tac-mxwireless ~]# systemctl start mariadb [root@tac-mxwireless ~]# systemctl enable mariadb ステップ 3: MariaDB の初期設定を行い、この DB を保護します。

[root@tac-mxwireless ~]#mysql_secure_installation

注:このスクリプトのすべての部分を実行します。実稼働環境で使用するすべての MariaDBサーバに推奨されます。各手順を注意深く読んでください。

In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none): OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation.

Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully! Reloading privilege tables.. ... Success! By default, a MariaDB installation has an anonymous user, allowing anyone to log into MariaDB without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment. Remove anonymous users? [Y/n] y ... Success! Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network. Disallow root login remotely? [Y/n] y ... Success! By default, MariaDB comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment. Remove test database and access to it? [Y/n] y - Dropping test database... ... Success! - Removing privileges on test database... ... Success! Reloading the privilege tables will ensure that all changes made so far will take effect immediately. Reload privilege tables now? [Y/n] y ... Success! Cleaning up... All done! If you've completed all of the above steps, your MariaDB installation should now be secure. Thanks for using MariaDB! ステップ4: freeRADIUSのデータベースを設定します(ステップ3で設定したパスワードを使 用します)。

[root@tac-mxwireless ~]# mysql -u root -p -e "CREATE DATABASE radius" [root@tac-mxwireless ~]# mysql -u root -p -e "show databases" [root@tac-mxwireless ~]# mysql -u root -p MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "radiuspassword"; MariaDB [(none)]> FLUSH PRIVILEGES; MariaDB [(none)]> \q Bye

CentOS 7 への PHP 7 のインストール

ステップ1:次のコマンドを実行して PHP7を CentOS7 にインストールします。

[root@tac-mxwireless ~]# cd ~ [root@tac-mxwireless ~]# curl 'https://setup.ius.io/' -o setup-ius.sh [root@tac-mxwireless ~]# sudo bash setup-ius.sh [root@tac-mxwireless ~]# sudo yum remove php-cli mod_php php-common [root@tac-mxwireless ~]# sudo yum -y install mod_php70u php70u-cli php70u-mysqlnd php70u-devel php70u-gd php70u-mcrypt php70u-mbstring php70u-xml php70u-pear [root@tac-mxwireless ~]# sudo apachectl restart

FreeRADIUS のインストール

ステップ1:次のコマンドを実行して、FreeRADIUS をインストールします。

[root@tac-mxwireless ~] # yum -y install freeradius freeradius-utils freeradius-mysql freeradiussqlite

ステップ2:mariadb.serviceの後にradius.serviceを開始します。

次のコマンドを実行します。

[root@tac-mxwireless ~]# vim /etc/systemd/system/multi-user.target.wants/radiusd.service [Unit] セクションに1行追加します。

After=mariadb.service

[Unit] セクションは次のように設定されている必要があります。

[Unit] Description=FreeRADIUS high performance RADIUS server. After=syslog.target network.target After=mariadb.service

ステップ 3:freeradius を開始し、起動時に開始できるようにします。

[root@tac-mxwireless ~]# systemctl start radiusd.service [root@tac-mxwireless ~]# systemctl enable radiusd.service ステップ4:セキュリティのため firewalld を有効にします。

[root@tac-mxwireless ~]# systemctl enable firewalld [root@tac-mxwireless ~]# systemctl start firewalld

[root@tac-mxwireless ~]# systemctl status firewalld

ステップ 5: http、https、および radius サービスを許可する永続的なルールをデフォルト ゾーン に追加します。

[root@tac-mxwireless ~]# firewall-cmd --get-services | egrep 'http|https|radius' [root@tac-mxwireless ~]# firewall-cmd --add-service={http,https,radius} --permanent success

ステップ6:変更を有効にするため、firewalldをリロードします。

[root@tac-mxwireless ~]# firewall-cmd --reload FreeRADIUS

MariaDB を使用するように FreeRADIUS を設定するには、次の手順に従います。

ステップ1:RADIUSデータベーススキームをインポートして、RADIUSデータベースを入力します。

[root@tac-mxwireless ~]# mysql -u root -p radius < /etc/raddb/modsconfig/sql/main/mysql/schema.sql

ステップ2:/etc/raddb/mods-enabledの下にStructured Query Language(SQL)用のソフト**リンクを** 作成します。

[root@tac-mxwireless ~]# ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/ ステップ3: SQL モジュール /raddb/mods-available/sql を設定し、ご使用の環境に合わせてデー タベース接続パラメータを変更します。

[root@tac-mxwireless ~]# vim /etc/raddb/mods-available/sql SQLセクションは次のようになります。

sql {

driver = "rlm_sql_mysql"
dialect = "mysql"

Connection info:

server = "localhost"

port = 3306 login = "radius" password = "radpass" # Database table configuration for everything except Oracle radius_db = "radius" } # Set to 'yes' to read radius clients from the database ('nas' table) # Clients will ONLY be read on server startup. read_clients = yes # Table to keep radius client info client_table = "nas"

ステップ 4: /etc/raddb/mods-enabled/sql のグループ権限を radiusd に変更します。

[root@tac-mxwireless ~]# chgrp -h radiusd /etc/raddb/mods-enabled/sql

FreeRADIUSでの認証、許可、アカウンティング(AAA)クライアントとしてのWLC

ステップ1:WLCの共有キーを設定するため、/etc/raddb/clients.conf を編集します。

[root@tac-mxwireless ~]# vim /etc/raddb/clients.conf ステップ2:下部に、コントローラのIPアドレスと共有キーを追加します。

client{ secret = shortname = }

WLC上のRADIUSサーバとしてのFreeRADIUS

GUI :

ステップ1:WLCのGUIを開き、図に示すように[SECURITY] > [RADIUS] > [Authentication] > [New]に移動します。

սիսիս		Save Configuration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	n Home
Security	RADIUS Authentication Servers	Apply New
AAA General	Auth Called Station ID Type 🛛 🗛 MAC Address:SSID 🛛 🗸	
 RADIUS Authentication 	Use AES Key Wrap 🗌 (Designed for FIPS customers and requires a key wrap compliant RADIUS server)	
Accounting	MAC Delimiter V	
DNS	Framed MTU 1300	

ステップ2:図に示すように、RADIUSサーバ情報を入力します。

RADIUS Authentication Serv	vers > New	
Server Index (Priority)	2 🗸	_
Server IP Address(Ipv4/Ipv6)	a.b.c.d	
Shared Secret Format	ASCII 🗸	•
Shared Secret	•••••	
Confirm Shared Secret	•••••	
Key Wrap	(Designed for	r FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812	
Server Status	Enabled \sim	
Support for CoA	Disabled \vee	
Server Timeout	10 seconds	
Network User	🗹 Enable	
Management	🗹 Enable	
Management Retransmit Timeout	2 seconds	
IPSec	Enable	

CLI :

> config radius auth add <index> <radius-ip-address> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
WLAN

GUI :

ステップ1:WLCのGUIを開き、図に示すように[WLANs] > [**Create New] > [**Goas]に移動します。

رابیان cisco	<u>m</u> onitor	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
WLANs	WLANs									
 ₩LANS WLANS Advanced 	Current Filt	er: Nor	ne [<u>Cha</u>	<u>nge Filter] [Cl</u>	<u>ear Filter]</u>			Create Ne	ew 🗸	Go

ステップ2:サービスセット識別子(SSID)とプロファイルの名前を選択して、図に示すように [Apply]をクリックします。

WLANs	> New			< Back	Apply
Туре		WLAN V	_		
Profile	Name	profile-name			
SSID		SSID-name			
ID		2 ~	•		

CLI :

> config wlan create <id> <profile-name> <ssid-name> ステップ3: WLAN に RADIUS サーバを割り当てます。

CLI :

> config wlan radius_server auth add <wlan-id> <radius-index> $\ensuremath{\mathsf{GUI}}$:

[**Security**] > [**AAA Servers]に移動**し、目的のRADIUSサーバを選択し、図のように[**Apply**]をクリッ クします。

WLANs > Edit 'ise-prof'	< Back	Apply
General Security QoS Policy-Mapping Advanced		
Layer 2 Layer 3 AAA Servers		
		^
RADIUS Servers		
RADIUS Server Overwrite interface		
Authentication Servers Accounting Servers EAP Parameters		
Enabled Enable Enable		
Server 1 IP:172.16.15.8, Port:1812 V None V		
Server 2 None V None V		
Server 3 None V None V		
Server 4 None V None V		
Server 5 None V None V		
Server 6 None V None V		
RADIUS Server Accounting		
Interim Update 📿 Interim Interval 0 Seconds		~
<	>	,

ステップ4:オプションでセッション時間を増やします。

CLI :

> config wlan session-timeout <wlan-id> <session-timeout-seconds> $\ensuremath{\mathsf{GUI}}$:

図に示すように、[Advanced] > [Enable Session Timeout]に移動し、[Apply]をクリックします。

WL	ANs > Edit 'ise-j	orof'				< Ba	ack	Apply
G	ieneral Securit	y QoS Policy-Mappin	g Adv	anced				
	Allow AAA Override	Enabled		DHCP		_		
	Coverage Hole Detection	🗹 Enabled		DHC	P Server	Override		
	Enable Session Timeout	Session Timeou (secs	;)	DHC Assi	P Addr. gnment	Required		
	Aironet IE	Enabled		OEAP				
	Diagnostic Channe <u>18</u>	Enabled		Spli	t Tunnel	Enabled		
	Override Interface ACL	IPv4 None 🗡	IPv6 None ∨	Manage	ement Frame P	Protection (MFP)		
	Layer2 Ad	None 🗸						
	URL ACL	None 🗸		MFP	Client Protection	on 🛃 Optional 🗸		
	P2P Blocking Action	Disabled V		DTIM P	eriod (in beaco	on intervals)		
	Client Exclusion ²	Enabled 60 Timeout Value (secs)	802.	11a/n (1 - 255	5) 1		
	Maximum Allowed Clients ^g	0		802. NAC	11b/g/n (1 - 2	255) 1		
<	Static IP Tunneling	□		NAC	State None	~1		> ×

ステップ 5:WLAN を有効にします.

CLI :

>	config	wlan	enable	<wlan-id></wlan-id>
G	UI:			

図に示すように、[General] > [Status] > [Tick Enabled] > [Apply]をクリックします。

dit 'ssid-na	ime'	< Back
Security	QoS Policy-Mapping Advanced	
e Name	ssid-name	
2	WLAN	
, ,	ssid-name	
tus	✓ Enabled	

freeRADIUS データベースへのユーザの追加

デフォルトでは、クライアントは PEAP プロトコルを使用しますが、freeRadius ではその他の方

式もサポートしています(このガイドでは説明しません)。

ステップ1:ファイル /etc/raddb/users を編集します。

[root@tac-mxwireless ~]# nano /etc/raddb/users ステップ2:ファイルの下部にユーザ情報を追加します。この例では、user1はユーザ名、 Cisco123はパスワードです。

user1 Cleartext-Password := <Cisco123> ステップ3: FreeRadius を再起動します。

[root@tac-mxwireless ~]# systemctl restart radiusd.service

freeRADIUS の証明書

FreeRADIUSには、デフォルトの認証局(CA)証明書と、パス/etc/raddb/certsに保存されているデ バイス証明書が付属していま*す。これらの証明書の名前*は、ca.pemとserver.pemです。 server.pemは、クライアントが認証プロセスを通過するときに受信する証明書です。EAP 認証に 異なる証明書を割り当てる必要がある場合は、これらの証明書を削除し、新しい証明書を正確に 同じ名前で同じパスに保存するだけで行えます。

エンド デバイスの設定

802.1x 認証と PEAP/MS-CHAP (Microsoft の Challenge-Handshake Authentication Protocol) バ ージョン 2 を使用して SSID に接続するように、ラップトップ Windows マシンを設定します。

WindowsマシンでWLANプロファイルを作成するには、次の2つのオプションがあります。

- 1. 認証を実行するため、freeRADIUS サーバの検証および信頼に使用する自己署名証明書をマ シンにインストールします。
- 2. RADIUS サーバの検証をバイパスし、認証の実行に使用するすべての RADIUS サーバを信頼します(これはセキュリティの問題となる可能性があるため、推奨されません)。 これらのオプションの設定については、「エンドデバイスの設定:WLANプロファイルの作成」を参照してください。

FreeRADIUS証明書のインポート

freeRADIUS にインストールされているデフォルト証明書を使用する場合は、次の手順に従い、 freeRADIUS サーバからエンド デバイスに EAP 証明書をインポートします。

ステップ1: FreeRadius から証明書を取得します。

----BEGIN CERTIFICATE----MIIE4TCCA8mgAwIBAgIJAKLmHn4eZLjBMA0GCSqGSIb3DQEBBQUAMIGTMQswCQYD VQQGEwJGUjEPMA0GA1UECBMGUmFkaXVzMRIwEAYDVQQHEwlTb21ld2hlcmUxFTAT BgNVBAoTDEV4YW1wbGUgSW5jLjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AZXhhbXBs ZS5jb20xJjAkBgNVBAMTHUV4YW1wbGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X DTE3MDMzMTExMTIxNloXDTE3MDUzMDExMTIxNlowgZMxCzAJBgNVBAYTAkZSMQ8w DQYDVQQIEwZSYWRpdXMxEjAQBqNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhh bXBsZSBJbmMuMSAwHqYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQG A1UEAxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwqqEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC0vJ53NN7J9vhpKhcB3B00XLpeQFWjqolQOB9F /8Lh2Hax2rzb9wxOi1MOyXR+kN22H7RNwUHET8VdyGUsA4OdZWuyz18sKi5H42GU Eu6GDw1YJvhHn4rVC36OZU/Nbaxj0eR8ZG0JGse4ftQKLfckkvCOS5QGn4X1elRS oFe27HRF+pTDHd+nzbaDvhYWvFoe6iA27Od7AY/sDuo/tiIJWGdm9ocPz3+0IiFC ay6dtG55YQOHxKaswH7/HJkLsKWhS4YmXLgJXCeeJqooqr+TEwyCDEaFaiX835Jp gwNNZ7X5US0Fcjuu0tpJJ3hfQ8K6uXjEWP0kDE0DAnqp4/n9AgMBAAGjggE0MIIB MDAdBgNVHQ4EFgQUysFNRZKpAlcFCEgwdOPVGV0waLEwgcgGA1UdIwSBwDCBvYAU ysFNRZKpAlcFCEgwdOPVGV0waLGhgZmkgZYwgZMxCzAJBgNVBAYTAkZSMQ8wDQYD VQQIEwZSYWRpdXMxEjAQBqNVBAcTCVNvbWV3aGVyZTEVMBMGA1UEChMMRXhhbXBs ZSBJbmMuMSAwHqYJKoZIhvcNAQkBFhFhZG1pbkBleGFtcGxlLmNvbTEmMCQGA1UE AxMdRXhhbXBsZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHmCCQCi5h5+HmS4wTAMBgNV HRMEBTADAQH/MDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuZXhhbXBsZS5j b20vZXhhbXBsZV9jYS5jcmwwDQYJKoZIhvcNAQEFBQADggEBACsPR2jiOFXnTsK4 lwnrrMylZZb12gDuqK+zKELox2mzlDMMK83tBsL8yjkv70KeZn821IzfTrTfvhzV mjX6HgaWfYyMjYYYSw/iEu2JsAtQdpvC3di10nGwVPHlzbozPdov8cZtCb21ynfY Z6cNjx8+aYQIcsRIyqA11XMOBwIXo141TOmoODdgfX951poLwgktRLkv17Y7owsz ChYDO++H7Iewsxx5pQfm56dA2cNrlTwWtMvViKyX7GlpwlbB0xgkLiFJ5+GFbfLh a0HBHZWhTKvffbr62mkbfjCUfJU4T3xgY9zFwiwT+BetCJgAGy8CT/qmnO+NJERO RUvDhfE =

----END CERTIFICATE-----

ステップ 2:前のステップでの出力をコピーし、テキスト ファイルに貼り付け、拡張子を .crt に 変更します。

ステップ3:ファイルをダブルクリックし、[Install Certificate...]を選択します。 図に示すように

Certificate 📰
General Details Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Example Certificate Authority
Issued by: Example Certificate Authority
Valid from 3/ 31/ 2017 to 5/ 30/ 2017
Install Certificate Issuer Statement
ок

ステップ4:図に示すように、証明書をTrusted Root Certification Authoritiesストアにインストー ルします。

Certificate Import Wizard	8
Certificate Store Certificate stores are system areas where certific	ates are kept.
Windows can automatically select a certificate sto the certificate. Automatically select the certificate store ba	re, or you can specify a location for used on the type of certificate
Place all certificates in the following store	
Certificate store:	Browse
Select Certificate Store	
Select the certificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Intrusted Certificates Show physical stores	Back Next > Cancel
OK Cancel	ОК

WLANプロファイルの作成

ステップ1:図に示すように、[スタート]アイコンを右クリック**し、[コン**トロールパネル]を選択 します。

Programs and Features	
Mobility Center	
Power Options	
Event Viewer	
System	
Device Manager	
Network Connections	
Disk Management	
Computer Management	
Command Prompt	
Command Prompt (Admin)	
Task Manager	
Control Panel	
File Explorer	
Search	
Run	
Shut down or sign out	>
Desktop	
iii ン に」 🔉 DownL 🦅 Networ	52

ステップ2:図に示すように、[Network and Internet] > [Network and Sharing Center] > [Set up a new connection or network]をクリックします。



ステップ3:[Manually connect to a wireless network]を選択し、図に示す[Nextas]をクリックします

	-		×
 Set Up a Connection or Network 			
Choose a connection option			
Connect to the Internet			1
Set up a broadband or dial-up connection to the Internet.			
Set up a new network			
Set up a new router or access point.			
Manually connect to a wireless network			
Connect to a hidden network or create a new wireless profile.			
Connect to a workplace			
Set up a dial-up or VPN connection to your workplace.			
			_
	Next	Car	ncel

ステップ4:SSIDの名前とセキュリティタイプWPA2-Enterpriseの情報を入力し、図に示すように [**Next**]をクリックします。

÷	Se Manually connect to a	wireless network	-		×	
	Enter information f	or the wireless network you want to add				
	Network name:	SSID-name				
	Security type:	WPA2-Enterprise ~				
	Encryption type:	AES.				
	Security Key:	Hide characte	HTS.			
	Start this connection	on automatically				
	Connect even if the network is not broadcasting					
	Warning: If you se	lect this option, your computer's privacy might be at ris	k.			
		,	lext	Can	cel	

ステップ5 : 図に示すようにWLANプロファイルの設定をカスタマイズするには、[Change connection settings]を選択します。

	-		\times
 Second Second Sec			
Successfully added ise-ssid			
→ Change connection settings			
Open the connection properties so that I can change the settings.			
		Clo	se

ステップ6:図に示すように、[セキュ**リティ]**タブに移動し**[設**定]をクリックします。

ise-ssid Wireless Ne	twork Properti	es		×
Connection Security				
Security type:	WPA2-Enterprise		\sim	
Encryption type:	AES		\sim	
Choose a network aut	thentication metho	1:	_	
Microsoft: Protected EAP (PEAP) V Settings				
Remember my credentials for this connection each time I'm logged on				
une in logged of				
	_			
Advanced settings				
	[OK	Cano	el

ステップ7:RADIUS サーバが有効になっているかいないか選択します。

検証する場合は [Verify the server's identity by validating the certificate] **を有効にし、[Trusted Root Certification Authorities:**] リストから freeRADIUS の自己署名証明書を選択します。

その後、[Configure]を選択し、[Automatically use my Windows logon name and password...]を無 効にして、図のように[OK]をクリックします。

Protected EAP Properties	×
When connecting:	
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):	
Trusted Root Certification Authorities:	
Digitie Stitchel Inner der Digitie Stitchel Association der Die der D	^
Example Certification Authority Construct Certification Authority Construct Certification Authority Solution	~
Notifications before connecting:	
Tell user if the server name or root certificate isn't specified	~
Select Authentication Method:	
Secured password (EAP-MSCHAP v2) Configur	е
Enable Fast Reconnect	
Disconnect if server does not present cryptobinding TLV Enable Identity Privacy	
OK Cance	el
EAP MSCHAPv2 Properties ×	

EAP MISCHAPVZ Properties			
When connecting:			
Automatically use my Windows logon name and password (and domain if any).			
ок	Cancel		

ステップ 8:ユーザ クレデンシャルを設定します。

[Security]タブに戻り、[Advanced settings] を選択し、[User authentication]として認証モードを指 定して、ユーザを認証するためにfreeRADIUSで設定したクレデンシャルを保存します。

ise-ssid Wireless Network Properties					
Connection Security					
Security type:	WPA2-Enterprise		~		
Encryption type:	AES		\sim		
Choose a network aut	thentication method	j:			
Microsoft: Protected EAP (PEAP) V Settings					
Remember my credentials for this connection each					
a dama da atta					
Advanced settings					
		OK	Cancel]	

_ open/ on new of the set		
User authentication	Save	credentials
Delete credentials for all use	ers	
Enable single sign on for this ne	twork	
Perform immediately before	e user logon	
 Perform immediately after u 	iser logon	
Maximum delay (seconds):	10	-
Allow additional dialogs to b sign on	e displayed during	g single
This network uses separate and user authentication	virtual LANs for m	achine

Windows Secu	ity		×
Save creder Saving your cre when you're no	ntials dentials allows your computer to connect to t logged on (for example, to download upo	o the network lates).	
ahahi	user1		
CISCO	••••••		
	OK	Cancel	

確認

ここでは、設定が正常に機能しているかどうかを確認します。

WCL での認証プロセス

特定のユーザの認証プロセスをモニタするため、次のコマンドを実行します。

> debug client <mac-add-client>

> debug dot1x event enable

> debug dot1x aaa enable

デバッグ クライアントの出力を簡単に読むための手段として、ワイヤレス デバッグ アナライザ ツールを使用します。

<u>ワイヤレス デバッグ アナライザ</u>

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。