Cisco Secure Services Client での PEAP/GTC WPA の設定例

内容

<u>概要</u> <u>前提条件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>Cisco Secure Services Client での PEAP/GTC WPA の設定</u> <u>ネットワークへの接続</u> <u>関連情報</u>

<u>概要</u>

このドキュメントでは、Cisco Secure Services Client で保護拡張認証プロトコル(PEAP)/汎用 トークン カード(GTC)Wi-Fi Protected Access(WPA)を設定する方法を説明します。

<u>前提条件</u>

<u>使用するコンポーネント</u>

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 Secure Services Client バージョン 4.0Cisco Secure Services Client は、<u>Cisco.com</u> <u>Software Center</u>(登録ユーザ専用)からダウンロードできます。
- Windows XP SP2 または 2000 SP 4 以上

<u>表記法</u>

ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してください。

<u>Cisco Secure Services Client での PEAP/GTC WPA の設定</u>

Cisco Secure Services Client に PEAP/GTC WPA を設定するには、次の手順を実行します。

1. Cisco Secure Services Client のシステム トレイ アイコンを右クリックし、[Open] を選択し ます。注:ネットワークに接続していない場合、システムトレイアイコンは暗くなります。 [Connect Enterprise] ダイアログボックスが表示されます。

ent Administration Help	
Create Networks Manage Networks	
Access A	Data Security
11 bandar	WEP
11 buffadeer	MPA WPA
21 c2g	B WPA
I Cisco1100	🙆 WPA
il cisco-beta1a	WEP
cisco-CTA2	WEP
CTA4	MPA WPA
ateway-AP	WEP
proxim	WEP
Create Netwo	Add to Network

- 2. [Create Networks] タブをクリックします。[Create Networks] 領域には、Service Set Identifier(SSID)をブロードキャストするネットワークが表示されます。
- 3. [Create Network] ボタンをクリックします。[Network Profile] ダイアログボックスが表示されます。

Network Profil	•	X
Network		
Name: demo_net	vork	
Availa	ble to all users (public profile)	
Autom	atically establish Machine conne	ction
Autor	atically establish User connectio	
	Before user account (supports si	artcard/password only)
Network Configurat	on Summary:	
Authentication:	Dff	
		Modify
Access Devices		
Access / SSID	Mode Notes	
Add	Modify Configuration	Remove
Help		OK Cancel

 [Network] 領域で、次のオプションを設定します。[Name] フィールドに、ネットワークの名前を入力します。この名前は、このネットワークの SSID として表示されます。この例では、この名前は demo_network です。[Available to all users (public profile)] チェックボックスをオンにします。[Automatically establish User connection] チェックボックスをオンにし、 [Automatically establish Machine connection] チェックボックスがオフであることを確認します。[Before user account (supports smartcard/password only)] チェックボックスをオンにします。注:[ユーザーアカウントの前に(スマートカードまたはパスワードのみをサポート)]チェックボックスがオンになっている場合、認証は資格情報の入力直後に、ドメインのログオンが発生する前に行われます。ユーザ証明書を使用しない場合は、[Before user account (supports smartcard/password only)] チェックボックスをオンにしないでください。ユーザ証明書は、Windows にログオンするまでは使用できないため、ユーザ証明書とドメインログオンを組み合わせて使用することはできません。 5. [Network Configuration Summary] エリアで [Modify] ボタンをクリックします。[Network Authentication] ダイアログボックスが表示されます。

Network: demo_network	
Authentication Methods:	Credentials:
🔿 Turn Off	 Request when needed
 Turn On Use Username as Identity Use 'Anonymous' as Identity 	 Remember forever Remember for this session Remember for 5 minutes
Protocol	 Use Single Sign on Credentials
FAST	
PEAP	
TTLS	
Configure	

 [Network Authentication] ダイアログ ボックスで次のオプションを構成します。[Credentials] エリアで [Use Single Sign on Credentials] オプション ボタンをクリックします。 [Authentication Methods] エリアで [Turn On] オプション ボタンをクリックしてから [Use 'Anonymous' as Identity] をクリックします。[Turn On] オプション ボタンをクリックすると 、[Authentication Methods] 領域に表示されるプロトコル リストにデータが入力されます。 [Use 'Anonymous' as Identity] オプション ボタンを押すと、リストは、トンネル化された認 証プロトコルのみに限定されます。[PEAP] チェックボックスをオンにして、[Configure] を クリックします。[Configure EAP Method] ダイアログボックスが表示されます。

Configure EAP Method		×
EAP settings:		
Use Client Certificate		
Validate Server Certificate		
Allow Fast Session Resumptio	n	
unneled Method		
GTC		
EAP-TLS Settings:		
Validate Server Certificate		
Allow Fast Session Resump	tion	

Client Certificate] チェック ボックスをオフにします。[Validate Server Certificate] チェック ボックスおよび [Allow Fast Session Resumption] チェックボックスをオンにします。 [Tunneled Method] ドロップダウン メニューから、[GTC] を選択します。[OK] をクリックし て [Network Authentication] ダイアログ ボックスに戻ってから、[OK] をクリックして [Network Profile] ダイアログ ボックスに戻ります。

7. [Network Profile] ダイアログ ボックスの [Access Devices] エリアで [Add] をクリックします。 [Add Access Device] ダイアログボックスが表示されます。

ACCESS -	Data Security	
<ethernet></ethernet>	Vired	
Atheros-AP2	NEP WEP	
Cisco1100	🔒 WPA	
00028a78b887 H	ligh Signal WPA	
i cisco-beta1a	WEP	
cisco-beta1g	C WEP	
cisco-CTA2	The WEP	
gateway-AP	WEP	
Actively search for this ac	ccess device	
Mode: WPA Enterprise	TKIP	~

- 8. [Add Access Devices] ダイアログ ボックスで、構成するデバイスを選択してから [Add Access] をクリックします。注:設定するデバイスが範囲内の場合、そのデバイスのSSIDが [Available Access Devices]リストに表示されます。デバイスが表示されない場合は、デバイ スの SSID を [Access (SSID)] フィールドに入力し、[Cisco 1100 Port Settings] 領域にポー ト設定を入力して [Add Access] をクリックします。
- 9. [Network Profile] ダイアログ ボックスで [OK] をクリックして [Connect Enterprise] ダイアロ グ ボックスに戻ります。
- 10. [Connect Enterprise] ダイアログ ボックスで [Client] メニューから [Trusted Servers] > [Manage Machine / All Users trusted servers] を選択します。[Manage Machine / All Users Trusted Servers] ダイアログ ボックスが表示されます。

ule Name	 Validation Method

11. [Add Server Rule] をクリックします。[Trusted Server] ダイアログ ボックスが表示されま

Contraction of the second second second	inv_nonvik			
Validation metho	od: Certificate	i,		
Atch ANY Cert	ificate Validatio	n Bule:		
Subject Alte	ernative Name	Ends with	~	mtgcorp.com
Subject/Co	mmon Name [Exactly matches	~	

- 12. [Trusted Server] ダイアログ ボックスで次のオプションを構成します。[Rule name] フィー ルドに、ルールの名前を入力します。[Validation method] ドロップダウン メニューから、 [Certificate] を選択します。[Match ANY Certificate Validation Rule] 領域で、ルールのオプ ションを設定します。ルールを作成するには、サーバ証明書の内容を知る必要があり、 [Match ANY Certificate Validation Rule] 領域にその値を入力します。たとえば、サブジェク トの別名にサーバのドメイン名 *mtgcorpserver.mtgcorp.com* が含まれている場合は、 [Subject Alternative Name] ドロップダウン メニューで [Ends with] を選択し、テキスト フ ィールドに **mtgcorp.com** を入力します。[OK] をクリックして [Manage Machine / All Users Trusted Servers] ダイアログ ボックスに戻ります。
- 13. [Manage Machine / All Users Trusted Servers] ダイアログ ボックスで、[Close] をクリック して [Connect Enterprise] ダイアログ ボックスに戻ります。

設定が完了したので、<u>ネットワークに接続</u>できます。

<u>ネットワークへの接続</u>

新規ネットワークに接続するには、次の手順を実行します。

1. [Connect Enterprise] ダイアログ ボックスで、[Manage Networks] タブをクリックします。

Connect Enter	prise		
ent Administration	n Help		
Create Networks	Manage Networks		
Network 🔺		Status	Data Security
· demo_	network	Disconnected	
HDCis	#1 Network	Connected	
, MDC	Cis#1	Connected	👸 WPA
<			>
Conne	ect Configure	Remove	Status
		₽.	

- 2. 新規ネットワークで使用するアダプタに接続しているすべてのネットワークへの接続を解除 します。
- 3. [Network] リストから新規ネットワーク プロファイルを選択し、[Connect] をクリックします。

設定および接続が正常に行われると、Cisco Secure Services Client のシステム トレイ アイコン が緑色で表示されます。

注:ウイルス対策ソフトウェアがコンピュータにインストールされ、Cisco Secure Services Clientログディレクトリを解析するように設定されている場合は、Cisco Secure Services Client認 証でCPUサイクルが長くなる可能性があります。パフォーマンスを向上するには、Cisco Secure Services Client のログ ディレクトリを除外するようにウイルス保護ソフトウェアを設定します。

関連情報

・<u>テクニカル サポートとドキュメント – Cisco Systems</u>