ネットワーク アクセスの拡張認証プロトコル (EAP)

[アーティクル] • 2023/03/09

> 適用対象: Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、Windows 10、Windows 8.1

拡張認証プロトコル (EAP) とは、IEEE 802.1X ベースのワイヤレス アクセス、IEEE 802.1X ベースのワイヤード アクセス、または仮想プライベート ネットワーク (VPN) などの Point-to-Point Protocol (PPP) 接続といったような一般的に使用される保護されたネットワーク アクセス テクノロジについて認証方法の拡張を実現するアーキテクチャ フレームワークです。 EAP は、MS-CHAP v2 などの認証方法ではなく、アクセス クライアントおよび認証サーバーにおけるフレームワークです。このフレームワークにより、ネットワーク ベンダーは EAP メソッドと呼ばれている新しい認証方法を開発し、容易にインストールすることができます。

認証方法

このトピックでは、EAP に含まれる次の認証方法に固有の構成情報について説明します。 トンネリングされた EAP メソッド内で使用される EAP 認証方法は、一般に**内部的な認証方法**または **EAP の種類**と呼ばれることに注意してください。

- [**保護された EAP (PEAP)**]

  このセクションでは、PEAP で提供される 2 つの既定の内部 EAP メソッドの構成について説明します。

  - EAP-TLS (トランスポート層セキュリティ)

    EAP-TLS は、オペレーティング システムで [**スマート カードまたはその他の証明書のプロパティ**] として表示され、PEAP の内部的な認証方法として、またはスタンドアロンの EAP メソッドとして展開できます。 内部的な認証方法として構成した場合の EAP-TLS の構成設定は、PEAP 内で動作するように構成することを除き、EAP-TLS を外部的な認証方法として展開するための設定と同じです。 構成の詳細については、「スマート カードまたはその他の証明書のプロパティの構成項目」を参照してください。

  - EAP-MS-CHAP v2 (Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2)

    セキュリティで保護されたパスワード EAP-MS-CHAP v2 は、パスワードによるネットワーク認証のために PEAP と併用することができる EAP の種類です。 EAP-MsCHAPv2 は、VPN のスタンドアロンの認証方法としても使用できますが、ワイヤレスの場合は PEAP の内部的な認証方法として使用することしかできません。

- **EAP-Tunneled TLS (TTLS)**

- **EAP-SIM (Subscriber Identity Module)、EAP-AKA (Authentication and Key Agreement)、および EAP-AKA' (AKA Prime)**

  SIM カードによる認証を有効にし、顧客がモバイル ネットワーク オペレーターからワイヤレス ブロードバンド サービス プランを購入すると実装されます。 通常、プランの一環として、SIM 認証用に事前に構成されたワイヤレス プロファイルが顧客に提供されます。

  ここでは、次の内容について説明します。
  - EAP-SIM の構成設定
  - EAP-AKA と EAP-AKA の構成設定

EAP-TLS、PEAP、および EAP-TTLS

802.1X で認証されたワイヤード (有線) アクセスとワイヤレス アクセス用の EAP のプロパティには、次の方法でアクセスできます。

- グループ ポリシーで、ワイヤード ネットワーク (IEEE 802.3) ポリシーおよびワイヤレス ネットワーク (IEEE 802.11) ポリシーの拡張を構成する。
- クライアント コンピューターで、ワイヤード (有線) 接続またはワイヤレス接続を手動で構成する。

仮想プライベート ネットワーク (VPN) 接続用の EAP のプロパティには、次の方法でアクセスできます。

- 接続マネージャー管理キット (CMAK) を使用して VPN 接続を構成する。
- クライアント コンピューター上で VPN 接続を手動で構成する。

802.1X 認証済みワイヤード アクセス、802.1X 認証済みワイヤレス アクセス、および VPN の場合、既定で、次のネットワーク認証方法用の EAP の設定を構成できます。

- Microsoft: スマート カードまたはその他の証明書 (EAP-TLS)
- Microsoft:保護された EAP (PEAP)
- Microsoft:EAP-TTLS

さらに、VPN の場合は、既定で MS-CHAP-V2 ネットワーク認証方法が利用できます。

保護された EAP のプロパティの構成設定

このセクションでは、保護された EAP 用に構成できる設定の一覧を示します。

> ⓘ **重要**
>
> PEAP と EAP に同じ種類の認証方法を使用すると、セキュリティが脆弱になります。 PEAP と (保護されていない) EAP の両方を展開する場合は、同じ種類の認証方法を使用しないでください。 たとえば、PEAP-TLS を展開する場合は、EAP-TLS を展開しないようにします。

証明書を検証してサーバーの ID を検証する

この項目では、クライアントがクライアント コンピューターに提示されたサーバーの証明書について、署名が正しいこと、有効期限が切れていないこと、および信頼されたルート証明機関 (CA) によって発行されたものであることを検証するように指定します。 既定の設定は [有効] です。**このチェック ボックスをオフにすると、クライアント コンピューターでの認証プロセス中にサーバーの ID が検証されません。サーバー認証を行わないと、許可されていないネットワークに知らずに接続してしまうなど、ユーザーは重大なセキュリティ上の危険にさらされます。**

[次のサーバーに接続する]

この項目では、ネットワークの認証および承認を行うリモート認証ダイヤルイン ユーザー サービス (RADIUS) サーバーの名前を指定できるようにします。 各 RADIUS サーバーの証明書の **[サブジェクト]** フィールドに表示されている名前を**正確**に入力するか、正規表現を使用してサーバー名を指定する必要があることに注意してください。 正規表現の完全な構文を使用してサーバー名を指定できますが、正規表現をリテラル文字列と区別するために、指定する文字列に "*" を少なくとも 1 つ含める必要があります。 たとえば、nps*.example.com と指定して、RADIUS サーバー nps1.example.com または nps2.example.com を指定できます。

RADIUS サーバーが指定されていない場合でも、RADIUS サーバーの証明書が信頼されたルート CA によって発行されたものであるかどうかがクライアントにより検証されます。

既定値:

- ワイヤードおよびワイヤレスの場合は有効になっていません。
- VPN の場合は有効になっています。

信頼されたルート証明機関

この項目では、信頼されたルート証明機関の一覧を表示します。 一覧は、コンピューターにインストールされている信頼されたルート CA およびユーザーの証明書ストアから作成されます。 サプリカントがサーバー (ネットワーク ポリシー サーバー (NPS) が実行されているサーバーやプロビジョニング サーバーなど) を信頼するかどうかを決定するために使用する、信頼されたルート CA 証明書を指定できます。 信頼されたルート CA が選択されていない場合は、RADIUS サーバーのコンピューター証明書が、インストールされている信頼されたルート CA によって発行されたものであるかどうかが 802.1X クライアントにより検証されます。 1 つ以上の信頼されたルート CA が選択されている場合は、RADIUS サーバーのコンピューター証明書が、選択されている信頼されたルート CA によって発行されたものであるかどうかが 802.1X クライアントにより検証されます。 信頼されたルート CA が選択されていない場合でも、RADIUS サーバーの証明書が信頼されたルート CA によって発行されたものであるかどうかがクライアントにより検証されます。

公開キー基盤 (PKI) がネットワーク上にあり、CA を使用して RADIUS サーバーに証明書を発行している場合は、信頼されたルート CA の一覧に CA 証明書が自動的に追加されます。

また、Microsoft 以外のベンダーから CA 証明書を購入することもできます。 Microsoft 以外の一部の信頼されたルート CA では、購入した証明書を **[信頼されたルート証明機関]** 証明書ストアに自動的にインストールするソフトウェアが提供されています。 この場合、この信頼されたルート CA は、信頼されたルート CA の一覧に自動的に表示されます。

> ⓘ **注意**
>
> クライアント コンピューターの **[現在のユーザー]** および **[ローカル コンピューター]** の **[信頼されたルート証明機関]** 証明書ストアにない信頼されたルート CA 証明書を指定しないでください。 クライアント コンピューターにインストールされていない証明書を指定すると、認証は失敗します。

既定では、有効になっていません (信頼されたルート CA は選択されていません)。

[接続前の通知]

この項目では、サーバー名またはルート証明書が指定されていない場合にユーザーに通知するかどうか、またはサーバー ID を検証するかどうかを指定します。

既定では、次のオプションが用意されています。

- ケース 1: **[新しいサーバーまたは信頼された CA を承認するときにユーザーに確認を求めません]** を選択すると、次のようになります。
  - サーバー名が **[次のサーバーに接続する]** の一覧に含まれていない場合
  - または、ルート証明書が見つかっても、**[PEAP のプロパティ]** の **[信頼されたルート証明機関]** の一覧で選択されていない場合
  - または、ルート証明書がコンピューター上にない場合

  ユーザーへの通知は行われず、接続は失敗します。

- ケース 2: **[サーバー名またはルート証明書が指定されなかった場合にユーザーに通知します]** を選択すると、次のようになります。
  - サーバー名が **[次のサーバーに接続する]** の一覧に含まれていない場合
  - または、ルート証明書が見つかっても、**[PEAP のプロパティ]** の **[信頼されたルート証明機関]** の一覧で選択されていない場合

  ルート証明書を承認するかどうかを確認するメッセージがユーザーに表示されます。 ユーザーが証明書を承認すると、認証が続行されます。 ユーザーが証明書を拒否すると、接続は失敗します。 このオプションでは、ルート証明書がコンピューター上に存在しない場合、ユーザーへの通知は行われず、接続は失敗します。

- ケース 3: **[サーバーの ID を検証できない場合にユーザーに通知します]** を選択すると、次のようになります。
  - サーバー名が **[次のサーバーに接続する]** の一覧に含まれていない場合
  - または、ルート証明書が見つかっても、**[PEAP のプロパティ]** の **[信頼されたルート証明機関]** の一覧で選択されていない場合
  - または、ルート証明書がコンピューター上にない場合

ルート証明書を承認するかどうかを確認するメッセージがユーザーに表示されます。 ユーザーが証明書を承認すると、認証が続行されます。 ユーザーが証明書を拒否すると、接続は失敗します。

認証方法を選択する

この項目では、ネットワーク認証の PEAP で使用する EAP の種類を選択できます。 既定では、**[セキュリティで保護されたパスワード (EAP-MSCHAP v2)]** と **[スマート カードまたはその他の証明書 (EAP-TLS)]** という 2 種類の EAP を使用できます。 ただし、EAP は EAP メソッドを追加できる柔軟性のあるプロトコルなので、これらの 2 つの種類に制限されるわけではありません。

詳細については次を参照してください:

- セキュリティで保護されたパスワード (EAP-MSCHAP v2) のプロパティの構成項目
- スマート カードまたはその他の証明書のプロパティの構成項目

既定では、[セキュリティで保護されたパスワード (EAP-MSCHAP v2)] になっています。

構成

この項目では、指定した EAP の種類のプロパティ設定にアクセスできます。

高速再接続を有効にする

セキュリティ アソシエーションが既に確立されている場合に、新しいまたは更新されたセキュリティ アソシエーションを効率よく (少ないラウンド トリップ回数で) 作成する機能を有効にします。

VPN 接続の場合、高速再接続では IKEv2 テクノロジを使用して、ユーザーが一時的にインターネットに接続できなくなった場合でも、シームレスで一貫した VPN 接続が可能です。 この機能は、ワイヤレス モバイル ブロードバンドを使用して接続するユーザーに最適です。

この利点のよくある例として、たとえば、電車で移動中に、ワイヤレス モバイル ブロードバンド カードを使用してインターネットに接続し、その後、企業ネットワークへの VPN 接続を確立する場合があります。

電車がトンネルを通過すると、インターネット接続が切断されます。 電車がトンネルを抜けると、ワイヤレス モバイル ブロードバンド カードはインターネットに自動的に再接続します。

高速再接続により、インターネット接続が再確立されると、アクティブな VPN 接続も自動的に再確立されます。 再接続は、数秒かかる場合もありますが、ユーザーに透過的に実行されます。

既定では、有効になっています。

ネットワーク アクセス保護を強制する

この項目では、ネットワークへの接続を許可する前に、EAP サプリカントがシステムの正常性の要件を満たしているかどうかを判断するために、サプリカントに対してシステムの正常性チェックを実行するように指定します。

既定では、有効になっていません。

[サーバーに暗号化バインドの TLV がない場合は切断する]

この項目では、RADIUS サーバーに暗号化バインドの Type-Length-Value (TLV) がない場合に、接続しているクライアントがネットワーク認証プロセスを終了するように指定します。 暗号化バインドの TLV は、内部的な認証方法と外部的な認証方法を組み合わせることによって、PEAP での TLS トンネルのセキュリティを向上させます。これにより、攻撃者は PEAP チャネルを使用して MS-CHAP v2 認証をリダイレクトすることによる man-in-the-middle 攻撃を行うことができなくなります。

既定では、有効になっていません。

ID プライバシーを有効にする (Windows 8 のみ)

クライアントが RADIUS サーバーを認証するまで ID を送信できないように構成するように指定します。オプションで匿名 ID の値を入力できます。 たとえば、**[ID プライバシーを有効にする]** チェック ボックスをオンにして、匿名 ID の値として「guest」と入力した場合、alice@example という ID を持つユーザーに対する ID 応答は guest@example になります。 **[ID プライバシーを有効にする]** チェック ボックスをオンにして、匿名 ID の値を指定しなかった場合、alice@example というユーザーに対する ID 応答は @example になります。

この設定は、Windows 8 以前のバージョンを実行しているコンピューターにのみ適用されます。

既定では、有効になっていません。

セキュリティで保護されたパスワードのプロパティの構成項目

[Windows のログオン名とパスワード (およびドメインがある場合はドメイン) を自動的に使う] チェック ボックスをオンにすると、ネットワーク認証の資格情報として、現在のユーザーの Windows サインイン名とパスワードを使うように指定します。

既定値:

- ワイヤードおよびワイヤレスの場合は有効になっています。
- VPN の場合は有効になっていません。

スマート カードまたはその他の証明書のプロパティの構成項目

このセクションには、EAP-TLS 用に構成できる項目が一覧表示されます。

[自分のスマート カードを使う]

この項目では、認証要求を行っているクライアントがネットワーク認証のためにスマート カードの証明書を提示することを指定します。

既定値:

- ワイヤードおよびワイヤレスの場合は有効になっていません。
- VPN の場合は有効になっています。

このコンピューターの証明書を使用する

この項目では、認証を行っているクライアントが、**[現在のユーザー]** または **[ローカル コンピューター]** の証明書ストアにある証明書を使用するように指定します。

既定値:

- ワイヤードおよびワイヤレスの場合は有効になっています。
- VPN の場合は有効になっていません。

単純な証明書の選択を使う (推奨)

この項目では、認証要件を満たす可能性が低い証明書が Windows によって除外されるようにするかどうかを指定します。 これにより、ユーザーに証明書の選択を求めるときに選択可能な証明書の数が絞り込まれます。

既定値:

- ワイヤードおよびワイヤレスの場合は有効になっています。
- VPN の場合は有効になっていません。

詳細設定

この項目では、**[証明書の選択を構成]** ダイアログ ボックスが開きます。 **[証明書の選択を構成]** ダイアログ ボックスの詳細については、「新しい証明書の選択の構成項目」を参照してください。

[証明書を検証してサーバーの ID を検証する]

この項目では、クライアントがクライアント コンピューターに提示されたサーバーの証明書について、署名が正しいこと、有効期限が切れていないこと、および信頼されたルート証明機関 (CA) によって発行されたものであることを検証するように指定します。 **このチェック ボックスをオフにしないでください。オフにすると、クライアント コンピューターでの認証プロセス中にサーバーの ID を確認できません。 サーバー認証を行わないと、許可されていないネットワークに知らずに接続してしまうなど、ユーザーは重大なセキュリティ上の危険にさらされます。**

既定では、有効になっています。

[次のサーバーに接続する]

この項目では、ネットワークの認証および承認を行う RADIUS サーバーの名前を指定できるようにします。 各 RADIUS サーバーの証明書の [サブジェクト] フィールドに表示されている名前を**正確**に入力するか、正規表現を使用してサーバー名を指定する必要があることに注意してください。 正規表現の完全な構文を使用してサーバー名を指定できますが、正規表現をリテラル文字列と区別するために、指定する文字列に "*" を少なくとも 1 つ含める必要があります。 たとえば、nps*.example.com と指定して、RADIUS サーバー nps1.example.com または nps2.example.com を指定できます。

RADIUS サーバーが指定されていない場合でも、RADIUS サーバーの証明書が信頼されたルート CA によって発行されたものであるかどうかがクライアントにより検証されます。

既定値:

- ワイヤードおよびワイヤレスの場合は有効になっていません。
- VPN の場合は有効になっています。

信頼されたルート証明機関

この項目では、**信頼されたルート証明機関**の一覧を表示します。 一覧は、コンピューターにインストールされている信頼されたルート CA およびユーザーの証明書ストアから作成されます。 サプリカントがサーバー (NPS を実行しているサーバー、プロビジョニング サーバーなど) を信頼するかどうかを決定するために使用する、信頼されたルート CA 証明書を指定できます。 信頼されたルート CA が選択されていない場合は、RADIUS サーバーのコンピューター証明書が、インストールされている信頼されたルート CA によって発行されたものであるかどうかが 802.1X クライアントにより検証されます。 1 つ以上の信頼されたルート CA が選択されている場合は、RADIUS サーバーのコンピューター証明書が、選択されている信頼されたルート CA によって発行されたものであるかどうかが 802.1X クライアントにより検証されます。

公開キー基盤 (PKI) がネットワーク上にあり、CA を使用して RADIUS サーバーに証明書を発行している場合は、信頼されたルート CA の一覧に CA 証明書が自動的に追加されます。

また、Microsoft 以外のベンダーから CA 証明書を購入することもできます。 Microsoft 以外の一部の信頼されたルート CA では、購入した証明書を **[信頼されたルート証明機関]** 証明書ストアに自動的にインストールするソフトウェアが提供されています。 この場合、この信頼されたルート CA は、信頼されたルート CA の一覧に自動的に表示されます。 信頼

されたルート CA が選択されていない場合でも、RADIUS サーバーの証明書が信頼されたルート CA によって発行されたものであるかどうかがクライアントにより検証されます。

クライアント コンピューターの **[現在のユーザー]** および **[ローカル コンピューター]** の **[信頼されたルート証明機関]** 証明書ストアにない信頼されたルート CA 証明書を指定しないでください。

> **注意**
>
> クライアント コンピューターにインストールされていない証明書を指定すると、認証は失敗します。

既定では、有効になっていません (信頼されたルート CA は選択されていません)。

証明書の表示

この項目では、選択した証明書のプロパティを表示できます。

[新しいサーバーまたは信頼された証明機関を承認するようユーザーに求めない]

この項目では、サーバーの証明書が正しく構成されていない場合、まだ信頼するように設定されていない場合、またはこれらの両方に該当する場合に、ユーザーはその証明書を信頼するように要求されなくなります。 ユーザー操作を簡素化するため、およびユーザーが攻撃者によって配置されるサーバーを誤って信頼しないようにするために、このチェック ボックスをオンにすることをお勧めします。

既定では、有効になっていません。

[この接続で別のユーザー名を使う]

この項目では、証明書のユーザー名と異なる認証用のユーザー名を使用するかどうかを指定します。

既定では、有効になっていません。

新しい証明書の選択の構成項目

[新しい証明書の選択] を使用して、認証の目的でクライアント コンピューター上で適切な証明書を自動的に選択するためにクライアント コンピューターが使用する条件を構成します。 その構成がワイヤード ネットワーク (IEEE 802.3) ポリシー、ワイヤレス ネットワーク (IEEE 802.11) ポリシー、または VPN 向けの接続マネージャー管理キット (CMAK) を介してネットワーク クライアント コンピューターに提供されると、指定した認証条件で、クライアントが自動的にプロビジョニングされます。

このセクションには、**[新しい証明書の選択]** の構成項目の一覧と、それぞれの説明が表示されます。

証明書の発行者

この項目では、証明書発行者によるフィルターを有効にするかどうかを指定します。

既定ではオフです。

[証明書発行者] の一覧

1 つまたは複数の証明書発行者を証明書に指定するときに使用します。

対応する認証機関 (CA) 証明書がローカル コンピューター アカウントの **[信頼されたルート証明機関]** または **[中間証明機関]** の証明ストアに存在する場合、すべての発行者の名前の一覧が表示されます。

- ルート証明機関と中間証明機関がすべて含まれます。
- コンピューターに存在する有効な証明書 (有効期限が切れていない証明書や失効していない証明書など) に対応する発行者のみが含まれます。

認証を許可する最終的な証明書の一覧には、この一覧で選択されたいずれかの発行者が発行した証明書のみが含まれます。

既定ではオフです。

[拡張キー使用法 (EKU)]

[すべての目的]、**[クライアント認証]**、**[任意の目的]**、またはこれらを組み合わせて選択できます。 組み合わせを選択すると、サーバーに対してクライアントを認証するために、3 つの条件の少なくとも 1 つを満たす証明書すべてが有効な証明書と見なされます。 EKU フィルターが有効になっている場合、1 つの項目を選択する必要があります。それ以外の場合は、**[OK]** コマンド コントロールが無効になります。

既定では、有効になっていません。

[すべての目的]

この項目では、オンにすると、サーバーに対してクライアントを認証するために、EKU が **[すべての目的]** になっている証明書が有効な証明書と見なされます。

既定では、オンになっています (**[拡張キー使用法 (EKU)]** チェック ボックスがオンになっている場合)。

クライアント認証

この項目では、オンにすると、サーバーに対してクライアントを認証するために、EKU が **[クライアント認証]** になっている証明書と、指定された一覧の EKU が有効な証明書と見なされます。

既定では、オンになっています (**[拡張キー使用法 (EKU)]** チェック ボックスがオンになっている場合)。

[任意の目的]

この項目では、オンにすると、EKU が **[任意の目的]** および一覧で指定された EKU になっているすべての証明書がクライアントからサーバーへの認証に有効な証明書と見なされます。

既定では、オンになっています (**[拡張キー使用法 (EKU)]** チェック ボックスがオンになっている場合)。

追加

この項目では、**[EKU の選択]** ダイアログ ボックスが開き、標準、カスタム、またはベンダー固有の EKU を **[クライアント認証]** または **[任意の目的]** の一覧に追加できます。

既定では、EKU が表示されていません。

削除

この項目では、選択した EKU を **[クライアント認証]** または **[任意の目的]** の一覧から削除します。

既定では、利用できません。

> **注意**

[証明書発行者] チェック ボックスと **[拡張キー使用法 (EKU)]** チェック ボックスの両方がオンになっている場合、両方の条件を満たす証明書のみがサーバーに対してクライアントを認証するために有効な証明書と見なされます。

[EKU の選択]

用意された一覧から EKU を選択したり、新しい EKU を追加したりできます。

項目	詳細
[追加]	**[EKU の追加/編集]** ダイアログ ボックスが開き、カスタム EKU を定義および追加できます。 **[下の一覧から EKU を選択してください]** で、一覧から EKU を選択して **[OK]** をクリックすると、選択した EKU が **[クライアント認証]** または **[任意の目的]** の一覧に追加されます。
[編集]	**[EKU の追加/編集]** ダイアログ ボックスが開き、追加したカスタム EKU を編集できます。 既定で事前に定義されている EKU は編集できません。
削除	**[EKU の選択]** ダイアログ ボックスの EKU の一覧から、選択したカスタム EKU を削除します。 既定で事前に定義されている EKU は削除できません。

[EKU の追加/編集]

項目	詳細
[EKU の名前を入力してください]	カスタム EKU の名前を入力する場所です。
EKU OID を入力してください	EKU の OID を入力する場所です。 数字、区切り記号、および "." のみを 使用できます。 ワイルド カードを使用でき、その場合、階層に含まれるすべての子 OID が許可されます。 たとえば、「1.3.6.1.4.1.311.*」と入力すると、1.3.6.1.4.1.311.42 および 1.3.6.1.4.1.311.42.2.1 が許可されます。

TTLS の構成項目

EAP-TTLS は、相互認証をサポートした標準ベースの EAP トンネリング方法で、EAP メソッドやその他の従来のプロトコルを使用することにより、クライアント包含認証に対してセキュリティ保護されたトンネルを提供します。 Windows Server 2012 での EAP-TTLS の導入により、EAP-TTLS をサポートする最もよく展開される RADIUS サーバーとの相互運用をサポートするために、クライアント側のサポートのみ提供されます。

このセクションには、EAP-TTLS 用に構成できる項目が一覧表示されます。

ID プライバシーを有効にする (Windows 8 のみ)

この項目では、クライアントが RADIUS サーバーを認証するまで ID を送信できないように構成するように指定します。 オプションで匿名 ID の値を入力できます。 たとえば、**[ID プライバシーを有効にする]** チェック ボックスをオンにして、匿名 ID の値として「guest」と入力した場合、alice@example という ID を持つユーザーに対する ID 応答は guest@example になります。 **[ID プライバシーを有効にする]** チェック ボックスをオンにして、匿名 ID の値を指定しなかった場合、alice@example というユーザーに対する ID 応答は @example になります。

この設定は、Windows 8 が実行されているコンピューターにのみ適用されます。

既定では、有効になっていません。

[次のサーバーに接続する]

この項目では、ネットワークの認証および承認を行う RADIUS サーバーの名前を指定できるようにします。 各 RADIUS サーバーの証明書の [サブジェクト] フィールドに表示されている名前を**正確**に入力するか、正規表現を使用してサーバー名を指定する必要があることに注意してください。 正規表現の完全な構文を使用してサーバー名を指定できますが、正規表現をリテラル文字列と区別するために、指定する文字列に "*" を少なくとも 1 つ含める必要があります。 たとえば、nps*.example.com と指定して、RADIUS サーバー nps1.example.com または nps2.example.com を指定できます。 RADIUS サーバーが指定されていない場合でも、RADIUS サーバーの証明書が信頼されたルート CA によって発行されたものであるかどうかがクライアントにより検証されます。

既定では、[なし] になっています。

信頼されたルート証明機関

この項目では、**信頼されたルート証明機関**の一覧を表示します。 一覧は、コンピューターにインストールされている信頼されたルート CA およびユーザーの証明書ストアから作成されます。 サプリカントがサーバー (NPS を実行しているサーバー、プロビジョニング サーバーなど) を信頼するかどうかを決定するために使用する、信頼されたルート CA 証明書を指定できます。 信頼されたルート CA が選択されていない場合は、RADIUS サーバーのコンピューター証明書が、インストールされている信頼されたルート CA によって発行されたものであるかどうかが 802.1X クライアントにより検証されます。 1 つ以上の信頼されたルート CA が選択されている場合は、RADIUS サーバーのコンピューター証明書が、選択されている信頼されたルート CA によって発行されたものであるかどうかが 802.1X クライアントにより検証されます。 信頼されたルート CA が選択されていない場合でも、RADIUS サーバーの証明書が信頼されたルート CA によって発行されたものであるかどうかがクライアントにより検証されます。

公開キー基盤 (PKI) がネットワーク上にあり、CA を使用して RADIUS サーバーに証明書を発行している場合は、信頼されたルート CA の一覧に CA 証明書が自動的に追加されます。 選択されている場合、ドメインにクライアント コンピューターを参加させると、ルート CA 証明書がそのコンピューターにインストールされます。

また、Microsoft 以外のベンダーから CA 証明書を購入することもできます。 Microsoft 以外の一部の信頼されたルート CA では、購入した証明書を **[信頼されたルート証明機関]** 証明書ストアに自動的にインストールするソフトウェアが提供されています。 この場合、この信頼されたルート CA は、信頼されたルート CA の一覧に自動的に表示されます。

クライアント コンピューターの **[現在のユーザー]** および **[ローカル コンピューター]** の **[信頼されたルート証明機関]** 証明書ストアにない信頼されたルート CA 証明書を指定しないでください。

> **注意**
>
> クライアント コンピューターにインストールされていない証明書を指定すると、認証は失敗します。

既定では、有効になっていません (信頼されたルート CA は選択されていません)。

[サーバーを承認できない場合に、ユーザーに確認しない]

この項目では (オンになっていない場合)、次のいずれかの理由によりサーバー証明書の検証に失敗したときに、サーバーを承認するか拒否するかを確認するメッセージが表示されます。

- **[信頼されたルート証明機関]** の一覧で、サーバー証明書のルート証明書が見つからないか、または選択されていない。
- 証明書チェーン内に 1 つ以上の中間ルート証明書が見つからない。
- サーバー証明書のサブジェクト名が、**[次のサーバーに接続する]** の一覧で指定されているサーバーのいずれとも一致しない。

既定ではオフです。

[認証に非 EAP メソッドを選択する]

認証に非 EAP と EAP のどちらの種類を使用するかを指定します。 **[認証に非 EAP メソッドを選択する]** を選択すると、**[認証に EAP メソッドを選択する]** が無効になります。 **[認証に非 EAP メソッドを選択する]** を選択すると、次の非 EAP の認証の種類がドロップダウン リストに表示されます。

- PAP
- CHAP
- MS-CHAP
- MS-CHAP v2

既定値:

- [認証に非 EAP メソッドを選択する] が有効になっています。
- 非 EAP の種類は PAP です。

[Windows のログオン名とパスワードを自動的に使う]

この項目では、オンにすると、Windows のサインイン資格情報を使用します。 このチェックボックスは、**[認証に非 EAP メソッドを選択する]** ボックスで **[MS-CHAP v2]** を選択した場合にのみ有効になります。 **PAP**、**CHAP**、および **MS-CHAP** を認証の種類に選択した場合は、**[Windows のログオン名とパスワードを自動的に使う]** は無効になります。

[認証に EAP メソッドを選択する]

この項目では、認証に EAP と非 EAP のどちらの種類を使用するかを指定します。 **[認証に EAP メソッドを選択する]** を選択すると、**[認証に非 EAP メソッドを選択する]** が無効になります。 **[認証に非 EAP メソッドを選択する]** を選択すると、既定では、次の非 EAP の認証の種類がドロップダウン リストに表示されます。

- Microsoft: スマート カードまたはその他の証明書
- Microsoft: MS-CHAP v2
- MS-CHAP
- MS-CHAP v2

> **注意**
>
> **[認証に EAP メソッドを選択する]** ボックスの一覧には、**PEAP** および **FAST** トンネル メソッドを除く、サーバーにインストールされているすべての EAP メソッドが列挙されます。 EAP の種類は、コンピューターによって検出された順序で表示されます。

構成

指定した EAP の種類のプロパティ ダイアログ ボックスが開きます。 既定の EAP の種類の詳細については、「スマート カードまたはその他の証明書のプロパティの構成項目」または「セキュリティで保護されたパスワード (EAP-MSCHAP v2) のプロパティの構成項目」を参照してください。

EAP-SIM の構成設定

EAP SIM (Subscriber Identity Module) は、GSM (Global System for Mobile Communications) の認証およびセッション キーの配布に使用されます。 EAP-SIM は RFC 4186 で定義されています。

次の表に、EAP-SIM の構成設定を示します。

Item	説明
[強力な暗号キーを使用する]	このチェック ボックスをオンにすると、プロファイルに強力な暗号化が使用されます。
[仮の ID を使用できる場合は、実際の ID をサーバーに送信しない]	このチェック ボックスをオンにすると、クライアントを介した固定 ID のサーバー要求に仮の ID が設定される場合、クライアントは認証に失敗します。 仮の ID は ID プライバシーに使用されます。そのため、ユーザーの実際の ID または固定 ID が認証時に公開されることはありません。
[領域の使用を有効にする]	領域名を入力する場所です。 **[領域の使用を有効にする]** をオンにした場合にこのフィールドを空白にすると、3GPP (3rd Generation Partnership Project) 標準の 23.003 V6.8.0 で説明されているように、領域 3gpp.org を使用して IMSI (International Mobile Subscriber Identity) から領域が派生します。
[領域の指定]	領域名を入力する場所です。

EAP-AKA の構成設定

UMTS (Universal Mobile Telecommunications System) の EAP AKA (Authentication and Key Agreement) は、UMTS USIM (Universal Subscriber Identity Module) を使用した認証およびセッション キーの配布に使用されます。 EAP AKA は RFC 4187 で定義されています。

次の表に、EAP-AKA の構成設定を示します。

Item	説明
[仮の ID を使用できる場合は、実際の ID をサーバーに送信しない]	このチェック ボックスをオンにすると、クライアントを介した固定 ID のサーバー要求に仮の ID が設定される場合、クライアントは認証に失敗します。 仮の ID は ID プライバシーに使用されます。そのため、ユーザーの実際の ID または固定 ID が認証時に公開されることはありません。
[領域の使用を有効にする]	領域名を入力する場所です。 **[領域の使用を有効にする]** をオンにした場合にこのフィールドを空白にすると、3GPP (3rd Generation Partnership Project) 標準の 23.003 V6.8.0 で説明されているように、領域 3gpp.org を使用して IMSI (International Mobile Subscriber Identity) から領域が派生します。
[領域の指定]	領域名を入力する場所です。

EAP-AKA の構成設定

EAP- AKA' (AKA Prime) は、EAP-AKA に変更を加えたバージョンで、次のように、3GPP 以外の標準を使用した 3GPP (3rd-Generation Partnership Project) ベースのネットワークへのアクセスを可能にするために使用されます。

- WiFi - これは Wireless Fidelity と呼ばれることもあります。
- EVDO (Evolution-Data Optimized)
- WiMax (Worldwide Interoperability for Microwave Access)

EAP-AKA' は RFC 5448 で定義されています。

次の表に、EAP-AKA の構成設定を示します。

Item	説明
[仮の ID を使用できる場合は、実際の ID をサーバーに送信しない]	このチェック ボックスをオンにすると、クライアントを介した固定 ID のサーバー要求に仮の ID が設定される場合、クライアントは認証に失敗します。 仮の ID は ID プライバシーに使用されます。そのため、ユーザーの実際の ID または固定 ID が認証時に公開されることはありません。
[領域の使用を有効にする]	領域名を入力する場所です。 **[領域の使用を有効にする]** をオンにした場合にこのフィールドを空白にすると、3GPP (3rd Generation Partnership Project) 標準の 23.003 V6.8.0 で説明されているように、領域 3gpp.org を使用して IMSI (International Mobile Subscriber Identity) から領域が派生します。
[領域の指定]	領域名を入力する場所です。

Item	説明
[ネットワーク名の不一致を無視する]	クライアントは、クライアントによって認識されるネットワーク名と、認証時に RADIUS サーバーによって送信された名前を比較します。 不一致がある場合、このオプションを選択すると無視されます。 このチェック ボックスをオフにした場合、認証に失敗します。
[高速再認証を有効にする]	高速再認証が有効になるように指定します。 高速再認証は、SIM 認証が頻繁に行われる場合に便利です。 完全な認証から派生する暗号化キーが再利用されます。 その結果、SIM アルゴリズムは認証が試行されるたびに実行する必要がなくなり、頻繁に試行される認証に伴うネットワーク操作の回数が減少します。とができます。

その他の技術情報

グループ ポリシーでの認証済みワイヤレス設定に関するその他の情報については、新しいワイヤレス ネットワーク (IEEE 802.11) ポリシー設定の管理に関するページを参照してください。

グループ ポリシーでの認証済みワイヤード設定に関するその他の情報については、新しいワイヤード ネットワーク (IEEE 802.3) ポリシー設定の管理に関するページを参照してください。

認証済みワイヤード アクセスおよび認証済みワイヤレス アクセスの詳細については、「 Advanced Security Settings for Wired and Wireless Network Policies」を参照してください。