インストール後の作業

この項では、Cisco Secure Access Control Server（ACS）Release 4.0 for Windows のインストール後の作業について説明します。

Windows 認証の設定

ACS で Windows データベースを使用してユーザ認証を行う場合は、信頼できるユーザ認証とグループ マッピングを行うために追加の設定が必要になります。要件は、ACS のインストール先がドメイン コントローラであるかメンバー サーバであるかによって異なります。

この項では、次のトピックについて取り上げます。

ドメイン コントローラ認証の設定

ACS がドメイン コントローラで実行されていて Windows ユーザ データベースを使用してユーザ認証を行う場合、必要な追加設定は、Windows ネットワーク構成に依存します。次に示すステップの中には、ACS がドメイン コントローラで実行される場合に常に適用可能なものが含まれています。ただし、特定の条件においてのみ必要なステップもあり、これらのステップについては、その説明の冒頭に注を示します。常に適用可能なステップ、および使用している Windows ネットワーク構成に適用可能なステップのみを実行するようにしてください。

ステップ 1　CISCO ワークステーションを追加します。

認証要求の Windows 要件を満たすには、ユーザのログイン先である Windows ワークステーションを ACS で指定する必要があります。ACS は、AAA クライアントによって送信される認証要求からこの情報を特定できないので、一般的なワークステーション名をすべての要求に使用します。*CISCO* をワークステーション名として使用します。

ローカル ドメイン、および ACS がユーザ認証に使用する信頼ドメインと子ドメインでは、次の条件を満たす必要があります。

- *CISCO* というコンピュータ アカウントが存在する。
- Windows によって認証されるすべてのユーザが、コンピュータ *CISCO* へのログイン権限を持っている。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 2　Server サービスのステータスを確認します。

ACS 認証サービスは、Microsoft Windows の標準サービスである Server サービスに依存します。ACS を実行するコンピュータで、Server サービスが実行され、その Startup Type が Automatic に設定されていることを確認します。

ヒント　Server サービスを設定するには、ローカル管理者アカウントを使用して ACS を実行するコンピュータにログインし、**Start > Programs Administrative Tools > Services** を選択します。サービスはアルファベット順に一覧表示されています。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 3　NTLM のバージョンを確認します。

（注）　このステップの操作は、ACS が、信頼ドメインまたは子ドメインに属するユーザを認証する場合にのみ必要です。ACS には変更が必要ありません。変更は Windows に対してだけです。

ACS は、LAN Manager（LM）、NTLM バージョン 1、または NTLM バージョン 2 のプロトコルを使用して、Windows クレデンシャルの認証をサポートしています。LM は最も弱いプロトコル、NTLM バージョン 2 は最も強いプロトコルと見なされています。1 つ以上のプロトコルをサポートできますが、次の条件を満たす必要があります。

a. 使用している NTLM のバージョンに関係なく、LAN Manager 認証レベルを設定する必要があります。適切な Windows セキュリティ ポリシー エディタで **Local Policies> Security Options** を選択します。**LAN Manager Authentication Level** ポリシーを特定し、このポリシーを設定します。たとえば、LM または NTLM バージョン 1 を使用している場合は、**Send LM & NTLM responses** に設定します。各種のオプションと NTLM バージョン 2 の設定の詳細については、該当する NTLM 認証レベルの資料を Microsoft Web サイトで参照してください。

b. 前の設定に加えて、NTLM バージョン 2 を使用する場合は、次の条件も満たす必要があります。

- ユーザ認証に関与する *各* Windows 2000 ドメイン コントローラが、Microsoft Web サイトにある Windows 2000 Service Pack 2 または Microsoft ホット フィックス KB893318 をインストールしている。

  または

- ユーザ認証に関与する *各* ドメイン コントローラが、Windows 2003 Service Pack 1 をインストールしている。このバージョンには、パッチが必要ありません。

ステップ 4　ユーザ アカウントを作成します。

ヒント　ACS をアップグレードまたは再インストールし、すでに前のインストール手順でユーザ アカウントを作成した場合は、別のユーザ アカウントを使用して ACS サービスを実行するときに限り、このステップを実行します。

ACS を実行するドメイン コントローラのドメインには、ACS サービスを実行するためのドメイン ユーザ アカウントが必要です（後のステップで説明します）。

a. ドメイン ユーザ アカウントを作成します。このユーザ アカウントは、ACS サービスを実行するために使用します。ユーザ アカウントには、ドメイン内の特定のグループ メンバーシップは必要ありません。

ヒント　ユーザ アカウントには、*ACSuser* のような認識しやすい名前を割り当てます。監査ポリシーをイネーブルにした場合、Event Viewer でこのユーザ名に関するエントリを参照すると、失敗した ACS 認証に関連する許可の問題をより簡単に診断できます。

作成したユーザ アカウントには、ACS の認証対象ユーザが含まれるすべての Active Directory フォルダに対して、**すべてのプロパティの読み取り**アクセス権を付与します。Active Directory フォルダに対するアクセス権を付与するには、Microsoft Management Console を使用して Active Directory にアクセスし、ACS によって認証されるユーザを含むフォルダのセキュリティ プロパティを設定します。

ヒント　ユーザの Active Directory フォルダのセキュリティ プロパティにアクセスするには、そのフォルダを右クリックし、**Properties** を選択して、Security タブを選択します。ユーザ名を追加するには **Add** をクリックします。

詳細については、『Windows 2000 Server Active Directory』を参照してください。

ステップ 5　ローカル セキュリティ ポリシーを設定します。

（注）　このステップの操作は、ACS が、信頼ドメインまたは子ドメインに属するユーザを認証する場合にのみ必要です。

ヒント　ACS をアップグレードまたは再インストールし、前のインストールですでにこの手順を実行している場合は、別のユーザ アカウントを使用して ACS サービスを実行するときに限り、このステップが必要です。

前のステップで作成したユーザ アカウントについて、次のローカル セキュリティ ポリシーにユーザを追加します。

- Act as part of the operating system
- Log on as a service

詳細については、P.2-10 の「ローカル セキュリティ ポリシーの設定」を参照してください。

ステップ 6　サービスを設定します。

（注）　このステップの操作は、ACS が、信頼ドメインまたは子ドメインに属するユーザを認証する場合にのみ必要です。

前のステップでセキュリティ ポリシーに追加したユーザとして実行されるように、すべての ACS サービスを設定します。

詳細については、P.2-13 の「ACS サービスの設定」を参照してください。

ステップ 7　NetBIOS をイネーブルにします。

ACS では、信頼ドメインまたは子ドメインのドメイン コントローラとの通信に NetBIOS が必要です。そのため、次において NetBIOS をイネーブルにする必要があります。

- ACS を実行するドメイン コントローラ
- ACS の認証対象ユーザを含む信頼ドメインのドメイン コントローラ
- ACS の認証対象ユーザを含む子ドメインのドメイン コントローラ

NetBIOS をイネーブルにするには、次の手順を実行します。

a. 各ドメイン コントローラ上でネットワーク接続の拡張 TCP/IP プロパティにアクセスします。

b. **WINS** タブをクリックします。

c. 適宜 NetBIOS を設定します。

詳細については、次の資料を参照してください。

- Microsoft.com にある『Install WINS in Windows 2000 Server or Windows 2000 Advanced Server』
- Microsoft.com にある『Install WINS in Windows Server 2003』

ステップ 8　DNS が正しく動作するようにします。

ACS が Active Directory でユーザ認証を行うためには、ネットワークで DNS が正しく動作している必要があります。RADIUS ベースのトークン サーバ認証や ACS Service Management イベント通知 E メールなど、その他の ACS 機能でも DNS を使用することがあります。IP アドレスでなくホスト名を使用するこれらの機能を設定している場合、DNS が正しく動作しないと、Active Directory に認証要求が送信されてもこれらの機能が正常に働かない可能性があります。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 9　DNS サフィックスを指定します。

（注）　このステップの操作は、ACS が、複数ドメインの Active Directory でユーザを認証する場合にのみ必要です。

ACS を実行するドメイン コントローラで、信頼ドメインや子ドメインそれぞれを DNS サフィックスとして一覧表示するように、ACS が使用するネットワーク接続を設定します。

a. ネットワーク接続の拡張 TCP/IP プロパティにアクセスします。

b. DNS タブを選択します。

c. 適宜 **Append these DNS suffixes** リストを設定します。

詳細については、次の資料を参照してください。

- Microsoft.com にある『Configure TCP/IP to use DNS』(Windows 2000)
- Microsoft.com にある『Configure TCP/IP to use DNS』(Windows 2003)

ステップ 10　WINS を設定します。

ACS で信頼ドメインまたは子ドメインに属するユーザを認証する必要があり、かつ ACS がそれらのドメインのドメイン コントローラとの接続に DNS を使用できない場合は、ネットワークで WINS をイネーブルにします。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 11　*LMHOSTS* ファイルを設定します。

（注）　このステップは、前の各ステップを実行した後で、信頼ドメインまたは子ドメインに属するユーザの Windows 認証やグループ マッピングが信頼できない場合にのみ実行します。

他のドメイン コントローラと確実に通信するための最終手段として、ACS を実行するドメイン コントローラで、ACS の認証対象ユーザが属する信頼ドメインまたは子ドメインの各ドメイン コントローラのエントリを含むように、*LMHOSTS* ファイルを設定します。

ヒント　*LMHOSTS* ファイルは非常に特殊な形式のファイルです。*LMHOSTS* ファイルの設定に関する要件を十分に理解しておく必要があります。

詳細については、次の資料を参照してください。

1. Microsoft.com にある『LMHOSTS File』
2. Windows オペレーティング システムに含まれている *LMHOSTS* ファイルのサンプル。デフォルトでは、このサンプル ファイルのパスは *<systemroot>\system32\drivers\etc\lmhosts.sam* になります。

メンバー サーバ認証の設定

ACS がメンバー サーバで実行されていて Windows ユーザ データベースを使用してユーザ認証を行う場合、必要な追加設定は、Windows ネットワーク構成に依存します。次に示すステップの多くは、ACS がメンバー サーバで実行される場合に常に適用可能です。ただし、特定の条件においてのみ必要なステップもあり、これらのステップについては、その説明の冒頭に注を示します。常に適用可能なステップ、および使用している Windows ネットワーク構成に適用可能なステップのみを実行するようにしてください。

ステップ 1　ドメイン メンバーシップを確認します。

Windows 認証ができない一般的な設定エラーの 1 つに、ユーザ認証に使用する Windows ドメインと同じ名前で、誤ってメンバー サーバがワークグループに割り当てられていることがあります。エラーであることは明白ですが、ACS を実行するコンピュータが正しいドメインのメンバー サーバであるかどうか確認することをお勧めします。

ヒント　コンピュータのドメイン メンバーシップを確認するには、Windows デスクトップで **My Computer** を右クリックし、**Properties** を選択します。次に **Network Identification** タブをクリックし、そのタブに記載されている情報を読みます。

ACS を実行するコンピュータが、展開計画で必要なドメインのメンバーになっていない場合は、この手順を進める前にこの状況を修正します。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 2　CISCO ワークステーションを追加します。

認証要求の Windows 要件を満たすには、ユーザのログイン先である Windows ワークステーションを ACS で指定する必要があります。ACS は、AAA クライアントによって送信される認証要求からこの情報を特定できないので、一般的なワークステーション名をすべての要求に使用します。*CISCO* をワークステーション名として使用します。

ローカル ドメイン、および ACS がユーザ認証に使用する信頼ドメインと子ドメインでは、次の条件を満たす必要があります。

- *CISCO* というコンピュータ アカウントが存在する。
- Windows によって認証されるすべてのユーザが、コンピュータ *CISCO* へのログイン権限を持っている。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 3　Server サービスのステータスを確認します。

ACS 認証サービスは、Microsoft Windows の標準サービスである Server サービスに依存します。ACS を実行するコンピュータで、Server サービスが実行され、その Startup Type が **Automatic** に設定されていることを確認します。

ヒント　Server サービスを設定するには、ローカル管理者アカウントを使用して ACS を実行するコンピュータにログインし、**Start > Programs Administrative Tools > Services** を選択します。サービスはアルファベット順に一覧表示されています。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 4　NTLM のバージョンを確認します。

（注）　このステップの操作は、ACS が、信頼ドメインまたは子ドメインに属するユーザを認証する場合にのみ必要です。ACS には変更が必要ありません。変更は Windows に対してだけです。

ACS は、LM、NTLM バージョン 1、または NTLM バージョン 2 のプロトコルを使用して、Windows クレデンシャルの認証をサポートしています。LM は最も弱いプロトコル、NTLM バージョン 2 は最も強いプロトコルと見なされています。1 つ以上のプロトコルをサポートできますが、次の条件を満たす必要があります。

a.　使用している NTLM のバージョンに関係なく、LAN Manager 認証レベルを設定する必要があります。適切な Windows セキュリティ ポリシー エディタで **Local Policies> Security Options** を選択します。**LAN Manager Authentication Level** ポリシーを特定し、このポリシーを設定します。たとえば、LM または NTLM バージョン 1 を使用している場合は、**Send LM & NTLM responses** に設定します。各種のオプションと NTLM バージョン 2 の設定の詳細については、該当する NTLM 認証レベルの資料を Microsoft Web サイトで参照してください。

b.　上記の設定に加えて、NTLM バージョン 2 を使用する場合は、次の条件も満たす必要があります。

— ユーザ認証に関与する各 Windows 2000 ドメイン コントローラが、Microsoft Web サイトにある Windows 2000 Service Pack 2 または Microsoft ホット フィックス KB893318 をインストールしている。

または

— ユーザ認証に関与する各ドメイン コントローラが、Windows 2003 Service Pack 1 をインストールしている。このバージョンには、パッチが必要ありません。

ステップ 5　ユーザ アカウントを作成します。

ヒント　ACS をアップグレードまたは再インストールし、すでにこの項目を実行している場合は、別のユーザ アカウントを使用して ACS サービスを実行するときに限り、このステップが必要です。

ACS を実行するドメイン コントローラのドメインには、ACS サービスを実行するためのドメイン ユーザ アカウントが必要です（後のステップで説明します）。

a. ドメイン ユーザ アカウントを作成します。このユーザ アカウントは、ACS サービスを実行するために使用します。ユーザ アカウントには、ドメイン内の特定のグループ メンバーシップは必要ありません。

ヒント　ユーザ　アカウントには、*ACSuser*　のような認識しやすい名前を割り当てます。監査ポリシーをイネーブルにした場合、Event Viewer でこのユーザ名に関するエントリを参照すると、失敗した ACS 認証に関連する許可の問題をより簡単に診断できます。

b. 作成したユーザ アカウントには、ACS の認証対象ユーザが含まれるすべての Active Directory フォルダに対して、**すべてのプロパティの読み取り**アクセス権を付与します。Active Directory フォルダに対するアクセス権を付与するには、Microsoft Management Console を使用して Active Directory にアクセスし、ACS によって認証されるユーザを含むフォルダのセキュリティ プロパティを設定します。

ヒント　ユーザの Active Directory フォルダのセキュリティ プロパティにアクセスするには、そのフォルダを右クリックし、**Properties** を選択して、**Security** タブをクリックします。ユーザ名を追加するには **Add** をクリックします。

詳細については、『Windows 2000 Server Active Directory』を参照してください。

ステップ 6　ローカル セキュリティ ポリシーを設定します。

前のステップで作成したユーザ アカウントについて、次のローカル セキュリティ ポリシーにユーザを追加します。

- Act as part of the operating system
- Log on as a service

詳細については、P.2-10 の「ローカル セキュリティ ポリシーの設定」を参照してください。

ステップ 7　サービスを設定します。

前のステップでセキュリティ ポリシーに追加したユーザとして実行されるように、すべての ACS サービスを設定します。

詳細については、P.2-13 の「ACS サービスの設定」を参照してください。

ステップ 8　NetBIOS をイネーブルにします。

ACS では、ユーザ認証要求の送信先であるすべてのドメイン コントローラとの通信に NetBIOS が必要です。そのため、次において NetBIOS をイネーブルにする必要があります。

- ACS を実行するメンバー サーバ
- ACS を含むドメインのドメイン コントローラ
- ACS の認証対象ユーザを含む信頼ドメインのドメイン コントローラ
- ACS の認証対象ユーザを含む子ドメインのドメイン コントローラ

NetBIOS をイネーブルにするには、次の手順を実行します。

- 各ドメイン コントローラ上でネットワーク接続の拡張 TCP/IP プロパティにアクセスします。
- **WINS** タブをクリックします。
- 適宜 NetBIOS を設定します。

詳細については、次の資料を参照してください。

- Microsoft.com にある『Install WINS in Windows 2000 Server or Windows 2000 Advanced Server』
- Microsoft.com にある『Install WINS in Windows Server 2003』

ステップ 9　DNS が正しく動作するようにします。

ACS が Active Directory でユーザ認証を行うためには、ネットワークで DNS が正しく動作している必要があります。RADIUS ベースのトークン サーバ認証や ACS Service Management イベント通知 E メールなど、その他の ACS 機能でも DNS を使用することがあります。IP アドレスでなくホスト名を使用するこれらの機能を設定している場合、DNS が正しく動作しないと、Active Directory に認証要求が送信されてもこれらの機能が正常に働かない可能性があります。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 10　DNS サフィックスを指定します。

（注）　このステップの操作は、ACS が、複数ドメインの Active Directory でユーザを認証する場合にのみ必要です。

ACS を実行するメンバー サーバで、各ドメインを DNS サフィックスとして一覧表示するように、ACS が使用するネットワーク接続を設定します。

a.　ネットワーク接続の拡張 TCP/IP プロパティにアクセスします。

b.　DNS タブを選択します。

c.　適宜 **Append these DNS suffixes** リストを設定します。

詳細については、次の資料を参照してください。

- Microsoft.com にある『Configure TCP/IP to use DNS』(Windows 2000)
- Microsoft.com にある『Configure TCP/IP to use DNS』(Windows 2003)

ステップ 11 WINS を設定します。

ACS で信頼ドメインまたは子ドメインに属するユーザを認証する必要があり、かつ ACS がそれらのドメインのドメイン コントローラとの接続に DNS を使用できない場合は、ネットワークで WINS をイネーブルにする必要があります。

詳細については、使用しているオペレーティング システムに関する Microsoft のマニュアルを参照してください。

ステップ 12 *LMHOSTS* ファイルを設定します。

（注） このステップは、前の各ステップを実行した後で、Windows 認証やグループ マッピングが信頼できない場合にのみ実行します。

ドメイン コントローラと確実に通信するための最終手段として、ACS を実行するメンバー サーバで、ACS の認証対象ユーザが属する各ドメイン コントローラのエントリを含むように、*LMHOSTS* ファイルを設定します。これには、子ドメインのドメイン コントローラが含まれます。

ヒント *LMHOSTS* ファイルは非常に特殊な形式のファイルです。*LMHOSTS* ファイルの設定に関する要件を十分に理解しておいてください。

詳細については、次の資料を参照してください。

- Microsoft.com にある『LMHOSTS File』
- Windows オペレーティング システムに含まれている *LMHOSTS* ファイルのサンプル。デフォルトでは、このサンプル ファイルのパスは *<systemroot>\system32\drivers\etc\lmhosts.sam* になります。

ローカル セキュリティ ポリシーの設定

始める前に

この手順は、次の条件のいずれかに該当する場合にのみ必要です。

- ACS がメンバー サーバ上で実行されていて、Windows ユーザ データベースを使用してユーザ認証を行う必要がある。
- ACS がドメイン コントローラ上で実行されていて、信頼ドメインまたは子ドメインに属するユーザの認証を行う必要がある。

ACS の実行に使用するユーザ アカウントは、すでに作成済みです。設定の要件の詳細については、P.2-6 の「メンバー サーバ認証の設定」または P.2-2 の「ドメイン コントローラ認証の設定」のうち、適切な手順を参照してください。

ローカル セキュリティ ポリシーを設定するには、次の手順を実行します。

ステップ 1　ローカル管理者アカウントを使用して、ACS を実行するコンピュータにログインします。

ステップ 2　**Start > Settings > Control Panel > Administrative Tools > Local Security Policy** を選択します。

ヒント　Start メニューで Control Panel が展開されない場合は、**Start > Settings > Control Panel** を選択します。**Administrative Tools** をダブルクリックし、次に **Local Security Policy** をダブルクリックします。

Local Security Settings ウィンドウが表示されます。

ステップ 3　Name カラムの **Local Policies** をダブルクリックし、次に **User Rights Assignment** をダブルクリックします。

Local Security Settings ウィンドウに、ポリシーおよびその関連設定のリストが表示されます。設定が必要なポリシーは次の 2 つです。

- Act as part of the operating system
- Log on as a service

ステップ 4　**Act as part of the operating system** ポリシーおよび **Log on as a service** ポリシーについて、次の手順を実行します。

a. ポリシー名をダブルクリックします。

Local Policy Setting ダイアログボックスが表示されます。

b. **Add** をクリックします。

Select Users or Groups ダイアログボックスが表示されます。

c. Add ボタンの下にあるボックスに、ユーザ アカウントのユーザ名を入力します。

（注）　ユーザ名は、ドメインを指定した形式であることが必要です。たとえば、*CORPORATE* ドメインに *ACSuser* という名前のユーザを作成した場合は、*CORPORATE\ACSuser* と入力します。

d. **Check Names** をクリックします。

Enter Network Password ダイアログボックスが表示されます。

e. 次の操作を実行します。

- **Connect as**：ドメインを指定したユーザ名を入力します。ユーザ名は、c. で指定したドメイン内に存在する必要があります。たとえば、指定したドメインが *CORPORATE* であり、*echamberlain* がそのドメイン内の有効なユーザである場合は、*CORPORATE\echamberlain* と入力します。
- **Password**：指定したユーザ アカウントのパスワードを入力します。**OK** をクリックします。

c. で指定したユーザ名が存在するかどうかが確認されます。Enter Network Password ダイアログボックスが閉じます。

f. Select Users or Groups ダイアログボックスで、**OK** をクリックします。

Select Users or Groups ダイアログボックスが閉じます。

ユーザ名が、Local Policy Setting ダイアログボックスの Assign To リストに追加されます。

g. **OK** をクリックします。

Local Policy Setting ダイアログボックスが閉じます。c. で指定済みの、ドメインを指定したユーザ名が、設定したポリシーに関連する設定に表示されます。

h. c. で指定したユーザ名が、修正したポリシーの Local Setting カラムに表示されていることを確認します。表示されていない場合は、これらの手順を繰り返します。

ヒント　追加したユーザ名を確認する際に、Local Setting カラムを広げる操作が必要な場合があります。

（注）　Effective Setting カラムは、動的には更新されません。この手順の後述のステップで、Effective Setting カラムに必要な情報が含まれていることを確認する方法を説明します。

Act as part of the operating system ポリシーと **Log on as a service** ポリシーの設定が完了すると、ユーザ アカウントが、設定したポリシーの Local Setting カラムに表示されます。

ステップ 5　変更したセキュリティ ポリシー設定が、ACS を実行するコンピュータに適用されていることを確認します。

a. Local Security Settings ウィンドウを閉じます。

Effective Setting カラムの情報をリフレッシュするには、ウィンドウを閉じます。

b. Local Security Settings ウィンドウを再び開きます。**Start > Programs > Administrative Tools > Local Security Policy** を選択します。

c. Name カラムの **Local Policies** をダブルクリックし、次に **User Rights Assignment** をダブルクリックします。

Local Security Settings ウィンドウに、ポリシーおよびその関連設定の更新済みリストが表示されます。

d. **Act as part of the operating system** ポリシーおよび **Log on as a service** ポリシーについて、ポリシーに追加したユーザ名が Effective Setting カラムに表示されていることを確認します。

（注）　ポリシーに含めるように設定したユーザ名が、両方のポリシーの Effective Setting カラムに表示されない場合は、ドメイン コントローラのセキュリティ ポリシー設定がローカル設定と矛盾する可能性があります。これら 2 つのポリシー設定に関してローカル設定が有効な設定となるように、ドメイン コントローラ上のセキュリティ ポリシーを設定して、矛盾を解決します。ドメイン コントローラ上のセキュリティ ポリシーの設定に関する詳細については、使用しているオペレーティング システムの Microsoft のマニュアルを参照してください。

ユーザ アカウントに、ACS サービスの実行と Windows 認証のサポートに必要な特権が割り当てられます。

ステップ 6　Local Security Settings ウィンドウを閉じます。

これで、指定したユーザ アカウントは、ACS サービスを正常に実行するために必要な権限を持つことができました。

ACS サービスの設定

始める前に

この手順は、次の条件のいずれかに該当する場合にのみ必要です。

- ACS がメンバー サーバ上で実行されていて、Windows ユーザ データベースを使用してユーザ認証を行う必要がある。
- ACS がドメイン コントローラ上で実行されていて、信頼ドメインまたは子ドメインに属するユーザの認証を行う必要がある。

ACS の実行に使用するユーザ アカウントはすでに作成済みで、ACS サービスを実行するために必要な権限を割り当ててあります。設定の要件の詳細については、P.2-6 の「メンバー サーバ認証の設定」または P.2-2 の「ドメイン コントローラ認証の設定」のうち、適切な手順を参照してください。

ACS サービスを設定するには、次の手順を実行します。

ステップ 1　ローカル管理者アカウントを使用して、ACS を実行するコンピュータにログインします。

ステップ 2　**Start > Settings > Control Panel > Administrative Tools > Services** を選択します。

ヒント　Start メニューで Control Panel が展開されない場合は、**Start > Settings > Control Panel** を選択します。**Administrative Tools** をダブルクリックし、次に **Services** をダブルクリックします。

Services ウィンドウに、サービス グループのリスト、および現在のグループに登録されているサービスすべてのリストが表示されます。サービス グループのリストは、左側の Tree リストにラベル付きで表示されます。現在のグループに登録されているサービスは、Tree リストの右側に表示されます。

ステップ 3　Tree リストで、**Services (local)** をクリックします。

ACS がインストールする Windows サービスは次のとおりです。

- CSAdmin
- CSAuth
- CSDbSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

ステップ 4　各 ACS サービスについて、次の手順を実行します。

a. サービスのリストで、ACS サービスを右クリックして、ショートカットメニューから **Properties** を選択します。

Computer Browser Properties (Local Computer) ダイアログボックスが表示されます。

b. **Log On** タブを選択します。

c. **This account** オプションを選択します。

d. **This account** オプションの横にあるボックスに、アカウントのユーザ名を入力します。

（注）　ユーザ名は、ドメインを指定した形式であることが必要です。たとえば、*CORPORATE* ドメインに *ACSuser* という名前のユーザを作成した場合は、**CORPORATE\ACSuser** と入力します。

e. **Password** ボックスと **Confirm Password** ボックスに、ユーザ アカウントのパスワードを入力します。

f. **OK** をクリックします。

すべての ACS サービスが、ユーザ アカウントの特権を使用して実行するように設定されます。

ステップ 5　すべての ACS サービスを再起動するには、次の手順を実行します。

a. ACS HTML インターフェイスにログインします。

b. **System Configuration** をクリックし、**Service Control** をクリックします。次に、ブラウザ ウィンドウの一番下にある **Restart** をクリックします。

CSAdmin を除く ACS サービスが再起動されます。

c. ACS サービスの再起動が完了するまで待ちます。完了するまでには、通常、1 ～ 2 分かかります。

d. ACS を実行するコンピュータのローカル管理者として続行し、**Start > Programs Administrative Tools > Services** を選択します。

e. Name カラムの **CSAdmin** をダブルクリックします。

CSAdmin Properties ダイアログボックスが表示されます。

f. **Stop** をクリックし、Service Control ダイアログボックスが閉じるまで待ちます。

g. **Start** をクリックし、Service Control ダイアログボックスが閉じるまで待ちます。

h. CSAdmin Properties ダイアログボックスで、**OK** をクリックします。

CSAdmin Properties ダイアログボックスが閉じます。

i. Services ウィンドウを閉じます。

ACS サービスが、指定したユーザ アカウントの特権を使用して実行されます。

ACS 3.x から 4.0 への ODBC ロギングの更新

以前に ACS 3.x ODBC ロギングを使用しており、データを保持したまま ACS 4.0 にアップグレードした場合、SQL テーブルが継続して機能するように ODBC テーブルを更新する必要があります。

SQL データベースに対する変更において、現在 ODBC フィールドはすべて、番号ではなく文字列で表示されます。フィールド タイプは、INTEGER から VARCHAR に変更されました。たとえば、`Message_Type VARCHAR(255) NULL` となります。

テーブルを再作成するには、次の手順を実行します。

ステップ 1　**System Configuration > Logging** を選択します。

Logging Configuration ページが表示されます。

ステップ 2　イネーブルにする ODBC ログの名前をクリックします。

ODBC log Configuration ページが表示されます。ここで、*log* は選択した ODBC ログの名前です。

ステップ 3　テーブルを作成するには、**Show Create Table** をクリックします。

ブラウザの右側に、Microsoft SQL Server の SQL Create Table 文が表示されます。テーブル名は、Table Name ボックスに指定されている名前です。カラム名は、Logged Attributes リストに指定されているアトリビュートです。

（注）　生成された SQL は、Microsoft SQL Server でのみ有効です。他のリレーショナル データベースを使用している場合、テーブルを作成するためのコマンドの記述方法については、使用しているリレーショナル データベースのマニュアルを参照してください。

ステップ 4　生成された SQL の情報を使用して、この ODBC ログに対するリレーショナル データベースのテーブルを作成します。

（注）　ODBC ロギングを機能させるためには、テーブル名とカラム名は生成された SQL にある名前と正確に一致している必要があります。

ステップ 5　**Log to ODBC accounting report** チェックボックスをオンにします。ここで、*log* は選択した ODBC ログの名前です。

ステップ 6　**Submit** をクリックします。

設定済みのシステム DSN を使用して指定されたリレーショナル データベースのテーブルに対して、ACS がロギング データの送信を開始します。

ステップ 7　各 ODBC ログについて、これまでのステップを繰り返します。

ログ設定の詳細については、『*User Guide for Cisco Secure ACS for Windows 4.0*』の「Logs and Reports」の章を参照してください。

ACS Solution Engine への移行

ACS for Windows から ACS Solution Engine への移行には、バックアップと復元の機能を使用します。ACS for Windows は ACS Solution Engine と互換性があるバックアップ ファイルを作成します。ただし、両者が同じバージョンの ACS ソフトウェアを使用している場合に限られます。

使用されている ACS for Windows のバージョン、およびそれが実行されているオペレーティング システムによって、移行のプロセスは異なります。たとえば、ACS が Windows NT 4.0 上で実行されている場合、この後の手順で、Windows 2000 Server へのアップグレードが必要であることが示されています。バックアップと復元の機能の使用は、同じバージョンの ACS 間でのみサポートされているため、ACS for Windows から ACS Solution Engine へデータを転送するには、ACS for Windows バージョン 4.0 を使用する必要があります。ACS for Windows バージョン 4.0 は、Windows 2000 Server および Windows Server 2003 をサポートしており、Windows NT 4.0 はサポート対象外です。

詳細については、以下の手順を参照してください。

始める前に

アップグレードやデータの転送を行う前に、元の ACS のバックアップを作成し、そのバックアップ ファイルを、ACS を実行しているコンピュータのローカル ドライブ以外の場所に保存します。

Windows バージョンの ACS から ACS Solution Engine へ移行するには、次の手順を実行します。

ステップ 1　『*Installation and Configuration Guide for Cisco Secure Access Control Server Solution Engine*』に記載されている手順に従って、アプライアンスを設定します。

ステップ 2　ACS for Windows をバージョン 4.0 にアップグレードします。バージョン 4.0 用のライセンスがない場合は、試用版を使用できます。試用版は、http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des で入手できます。

ACS を Windows NT 4.0 上で実行している場合は、まず ACS バージョン 3.0 にアップグレードします。次に、Windows 2000 Server へ移行してから、ACS バージョン 4.0 にアップグレードします。ACS バージョン 4.0 は Windows NT 4.0 をサポートしていません。ACS バージョン 3.0 は、Windows NT 4.0 をサポートする ACS の最新バージョンです。ACS バージョン 3.0 へのアップグレードや Windows 2000 Server への移行については、『*Installing Cisco Secure ACS 3.0 for Windows 2000/NT Servers*』を参照してください。ACS バージョン 3.0 の試用版は、http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des でダウンロードできます。

（注）　アップグレード プロセスのテストを行った ACS のバージョンについては、リリース ノートを参照してください。最新バージョンのリリース ノートは Cisco.com で入手できます。URL は次のとおりです。
http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html

ステップ 3　ACS for Windows バージョン 4.0 の HTML インターフェイスで、ACS Backup 機能を使用して、データベースのバックアップを作成します。ACS Backup 機能の詳細については、『*User Guide for Cisco Secure ACS for Windows 4.0*』を参照してください。

ステップ 4　ACS for Windows バージョン 4.0 を実行しているコンピュータから FTP サーバ上のディレクトリに、バックアップ ファイルをコピーします。このディレクトリは FTP のルート ディレクトリからアクセス可能である必要があります。ACS Solution Engine は、この FTP サーバに接続可能である必要があります。ゲートウェイ デバイスでは、アプライアンスと FTP サーバとの間の FTP 通信が許可されていることが必要です。

ステップ 5　ACS Solution Engine の HTML インターフェイスで、ACS Restore 機能を使用して、データベースを復元します。データベースの復元の詳細については、『*User Guide for Cisco Secure Access Control Server Solution Engine*, version 4.0』を参照してください。

ACS Solution Engine に、移行元となった Windows バージョンの ACS の元の構成が含まれます。

ステップ 6　引き続き ACS Solution Engine の HTML インターフェイスで、Proxy Distribution Table の **(Default)** エントリの設定が正しいことを確認します。**Network Configuration** > **(Default)** を選択し、Forward To リストにそのアプライアンスのエントリが含まれるようにします。

ステップ 7　ACS for Windows を実行しているコンピュータの代わりに ACS Solution Engine を使用する場合は、アプライアンスの IP アドレスを、ACS for Windows を実行しているコンピュータの IP アドレスに変更する必要があります。

（注）　ACS Solution Engine の IP アドレスを、ACS for Windows を実行するコンピュータのアドレスに変更しない場合、ACS Solution Engine の IP アドレスを使用するには、すべての AAA クライアントの再設定が必要になります。

ACS Solution Engine の IP アドレスを変更するには、次の手順を実行します。

a.　ACS for Windows を実行するコンピュータの IP アドレスを記録します。

b.　Windows 上で ACS を実行するコンピュータの IP アドレスを別の IP アドレスに変更します。

c.　ACS Solution Engine の IP アドレスを、ACS for Windows を実行するコンピュータが以前使用していた IP アドレスに変更します。これは、a. で記録した IP アドレスです。詳細な手順については、『*Installation and Configuration Guide for Cisco Secure Access Control Server Solution Engine*』を参照してください。

ACS のアンインストール

Windows の Control Panel 機能である Add/Remove Programs を使用して、ACS ソフトウェアをインストールされているコンピュータから削除できます。ACS を削除すると、それが提供していた AAA サービスも当然、実行されていたコンピュータで使用できなくなります。

（注） Add/Remove Programs 機能を使用できない場合（ACS が正しくインストールされなかったか正しく削除されなかった、またはその他の障害がある場合）、ACS の CD にある **clean.exe** プログラムを特定し、ACS のインストールに障害があるコンピュータ上で実行します。**clean.exe** プログラムを実行すると、ACS は完全に削除されます。

始める前に

ACS ディレクトリ内のディレクトリにアクセスしているアプリケーションやコマンド ウィンドウをすべて閉じます。他のプロセスが ACS ディレクトリやそのサブディレクトリを使用していると、インストールは成功しません。たとえば、Windows Explorer が ACS ディレクトリの内容を表示していると、インストールは失敗します。

ACS をアンインストールするには、次の手順を実行します。

ステップ 1　ローカル管理者アカウントを使用して、ACS をアンインストールするコンピュータにログインします。

ステップ 2　**Start > Settings > Control Panel > Add/Remove Programs** を選択します。

ヒント　Start メニューで Control Panel が展開されない場合は、**Start > Settings > Control Panel** を選択します。次に、**Add/Remove Programs** をダブルクリックします。

Add/Remove Programs ウィンドウが表示されます。

ステップ 3　Currently installed programs リストから、**Cisco Secure ACS v*x.x*** を選択します。ここで、*x.x* は、コンピュータにインストールされている ACS のバージョンです。

ステップ 4　**Change/Remove** をクリックします。

Confirm File Deletion ダイアログボックスが表示されます。

ステップ 5　**Yes** をクリックします。

アンインストールが開始されます。

ステップ 6　ダイアログボックスに次のメッセージが表示されます。

```
The Cisco Secure ACS Service is currently running.
If you still want to continue the uninstall, it will be
stopped for you.
```

Continue をクリックします。

（注）　**Abort Uninstall** をクリックすると、アンインストールは停止します。ACS はまだコンピュータにインストールされている状態です。アンインストールが失敗した場合は、ACS の CD にある **clean.exe** プログラムを特定し、ACS のインストールに障害があるコンピュータ上で実行します。

アンインストールが続行されます。ACS サービスが停止します。

ステップ 7　ダイアログボックスに次のメッセージが表示されます。

```
You might choose to keep the existing ACS internal database,
which will save time if you reinstall the software at a later date.
```

- ACS 内部データベースのユーザとグループのデータを保持するには、**Keep Database** をクリックします。ユーザとグループの設定は、ACS がインストールされたディレクトリに保存されます。

注意　その他の設定は保存されません（ユーザとグループのデータだけ保存されます）。その他の設定データを保存するには、最初にバックアップを実行します。P.1-6 の「バックアップ データ」または『*User Guide for Cisco Secure ACS for Windows 4.0*』に記載のバックアップ手順を参照してください。

パスワードを入力するように求められます。このパスワードは、インストールのインポート ステップで使用します。今後のインストールのインポート フェーズ用、またはテクニカル サポートがデータベースにアクセスする必要がある場合に備えて、このパスワードを安全な場所に保存しておいてください。

- ACS 内部データベースを保持しない場合は、**Delete Database** をクリックします。

注意　**Delete Database** を選択し、データベースのバックアップも作成していないと、ユーザおよびグループのデータは消失します。

アンインストールが終了します。

ステップ 8　**OK** をクリックします。

次の作業

インストールが完了したら、ネットワークで ACS を展開する多種多様なオプションが用意されています。

提案されている展開シーケンスおよび ACS 製品機能の活用方法については、『*User Guide for Cisco Secure ACS for Windows 4.0*』の「Deployment Considerations」を参照してください。バックアップや復元、証明書のセットアップ、およびその他の重要な作業など、すべての管理機能の詳細についても、『*User Guide for Cisco Secure ACS for Windows 4.0*』を参照できます。

最新情報については、Cisco.com でリリース ノートを参照してください。

システムへのログインおよびシステムからのログアウト

ACS にアクセスするには、次の手順を実行します。

ステップ 1　マシンの Uniform Resource Locator（URL）を次のように指定して、ブラウザを開きます。

- http://*IP address*:2002
- http://*hostname*:2002

ここで、*IP address* は ACS を実行するコンピュータのドット付き 10 進数の IP アドレスで、*hostname* は ACS を実行するコンピュータのホスト名です。ホスト名を使用する場合、ネットワークで DNS が正常に機能しているか、ブラウザを実行しているコンピュータにあるローカル ホスト ファイルにそのホスト名が記載されていることが必要です。

管理セッションの保護のために SSL を使用するように ACS が設定されている場合でも、URL に HTTPS プロトコルを指定することで、HTML インターフェイスにアクセスできます。

- https://*IP address*:2002
- https://*hostname*:2002

ステップ 2　ACS ログイン ページで、ログインするための有効なユーザ名とパスワードをログイン画面に入力し、**Login** をクリックします。

ステップ 3　ログオフするには、ブラウザ ウィンドウの右上隅にある **X** をクリックします。ページがリフレッシュしたら、**Logoff** をクリックします。

HTML インターフェイスへのログインおよびアクセスの詳細については、『*User Guide for Cisco Secure ACS or Windows 4.0*』を参照してください。

ソフトウェア バージョン情報の表示

ACS ソフトウェア バージョン情報は、HTML インターフェイスの最初のログイン ページの下部に表示されます。HTML インターフェイスを使用している場合は、HTML インターフェイスの右上隅にある **X** をクリックして、ログイン ページに戻ることができます。次に、ソフトウェア バージョンと著作権情報の一部の例を示します。

```
Cisco Secure ACS
Release 4.0(1) Build xx
Copyright ©2005 Cisco Systems, Inc.
```