CHAPTER 5

アクセス ポリシーの設定

RADIUS アクセス ポリシーは、ユーザやユーザ グループにネットワークへのアクセス権が付与される前に ACS Express サーバが受信する RADIUS 認証要求を処理するために設定された選択規則、認証規則、および結果を集めたものです。ネットワークに接続されているデバイスに使用する TACACS+ 要求には同様のアクセス ポリシーがあります。

選択規則を使用して、アクセス要求で必要な送信デバイス、RADIUS 要求アトリビュートと値などの情報を指定します。認証規則には、ユーザの認証に使用するデータベース、使用するプロトコル、ユーザ グループ メンバーシップやアクセスの時刻などのポリシー要素が含まれます。結果には、特定のアクセス サービスに付与するエンタイトルメントを指定します。

ネットワーク アクセス ポリシーは、無線、有線、または VPN ネットワークにアクセスしようとするユーザに適用されます。ネットワーク アクセス ポリシーでも、PAP、CHAP、MSCHAPv2、PEAP、EAP-TLS、EAP-FAST、LEAP、Windows マシン認証などのさまざまな認証スキームがサポートされます。ネットワーク アクセス ポリシーは、RADIUS を使用して ACS Express と通信するネットワーク デバイスに適用されます。ネットワーク アクセス ポリシーは、Active Directory、LDAP、One-Time Password（OTP; ワンタイム パスワード）データベース、または ACS Express の内部ユーザ データベースに対してユーザ認証を行うように設定できます。

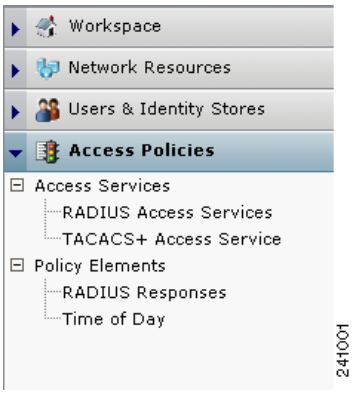
デバイス管理ポリシーは、ネットワーク デバイスにアクセスして設定しようとするユーザに適用されます。ACS Express は、ユーザに対して最大限許可される特権レベルの認証および認可を行います。ネットワーク デバイスが ACS Express と通信するときには、TACACS+ または RADIUS を使用します。デバイス管理ポリシーは、Active Directory、LDAP、ワンタイム パスワード データベース、または ACS Express の内部ユーザ データベースに対してユーザ認証を行うように設定できます。

この章は、次の内容で構成されています。

- 「アクセス サービス」（P.5-2）
  - 「RADIUS アクセス サービス」（P.5-2）
  - 「TACACS+ アクセス サービス」（P.5-8）
- 「ポリシー要素」（P.5-12）
  - 「RADIUS 応答」（P.5-12）
  - 「時間帯」（P.5-14）

図 5-1 は、ACS Express GUI のアクセス ポリシー ドロワーを示したものです。

図 5-1　アクセス ポリシー ドロワー



アクセス サービス

ACS Express は、次の 2 種類のアクセス サービスをサポートします。

- RADIUS アクセス サービス
- TACACS+ アクセス サービス

RADIUS アクセス サービス

ACS Express は RADIUS アクセス サービスを使用して、ログインを試行するユーザ クレデンシャルの確認方法についての規則を設定します。RADIUS アクセス サービスには、次の要素を設定します。

- ステータス
  - 名前
  - ステータス
- 選択規則
  - 利用可能なデバイス グループの割り当て
  - RADIUS 要求アトリビュートの割り当て
- 結果
  - 認証データベースの選択
  - EAP 方式の選択
  - セッション認可規則の設定

この項は、次の内容で構成されています。

- 「RADIUS アクセス サービスの追加」（P.5-3）
- 「RADIUS アクセス サービスの編集」（P.5-7）
- 「RADIUS アクセス サービスのコピー」（P.5-8）

- 「RADIUS アクセス サービスの削除」（P.5-8）

RADIUS アクセス サービスの追加

RADIUS アクセス サービスを追加するには、次の手順を実行します。

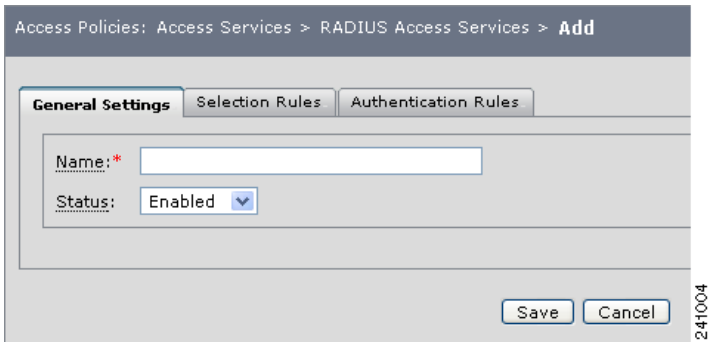
ステップ 1　[Access Policies] を選択し、[Access Services] 下の [RADIUS Access Services] を選択します。

[Access Policies: Access Services] > [RADIUS Access Services] ウィンドウに、現在定義されている RADIUS アクセス サービスが表示されます。

ステップ 2　[Add] をクリックします。

[Add RADIUS Access Services] ウィンドウ（図 5-2）に、[General Settings] タブが表示されます。

図 5-2　RADIUS アクセス サービスの追加



ステップ 3　RADIUS アクセス サービスの名前を入力します。

ステップ 4　この RADIUS アクセス サービスを無効にするには、プルダウン メニューを使用して、ステータスを [Disabled] にします。それ以外の場合は、デフォルトのステータス [Enabled] をそのまま受け入れます。

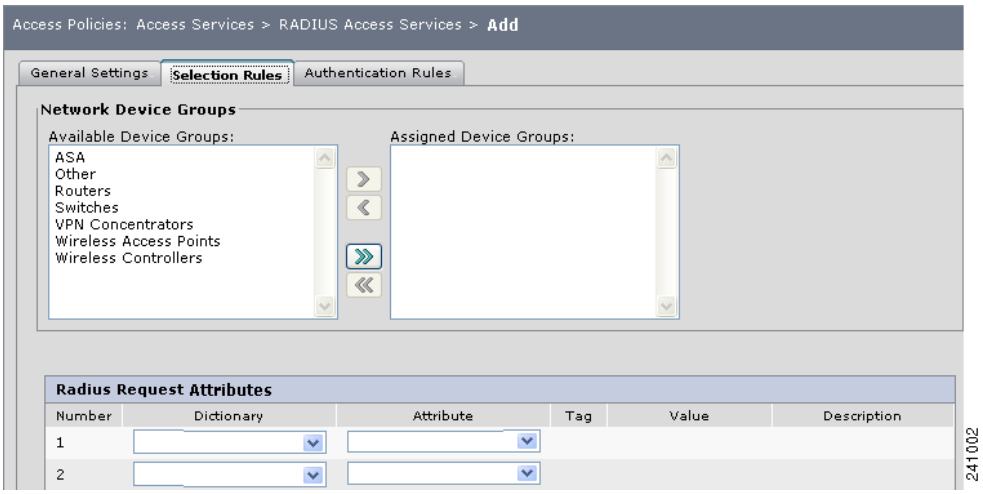
ステップ 5　[Selection Rules] タブをクリックします。

[Selection Rules] ウィンドウ（図 5-3）を使用して、アクセス要求を受信する [Network Device Groups] を設定し、着信の RADIUS アクセス要求で受け取る [RADIUS Request Attributes] を指定します。着信の RADIUS アクセス要求が、[Results] ウィンドウで指定する動作を実行できるようにするには、このウィンドウに設定した条件と一致する必要があります。

RADIUS アクセス サービスは、要求アクセスを送信する可能性のあるデバイスの種類ごとに作成することが必要です。たとえば、無線環境では、無線アクセス ポイントと無線コントローラ用の RADIUS アクセス サービスを設定する必要があります。VPN アクセスが許可されているサイトでは、VPN コンセントレータの RADIUS アクセス サービスを設定してください。

RADIUS アクセス サービスごとに、[Network Device Groups] で少なくとも 1 つの [Available Device Groups] を割り当てることが必要です。いずれかの [Available Device Groups] をクリックして選択し、大なりボタン（>）をクリックして、該当の RADIUS アクセス サービスに、選択したデバイス グループを割り当てます。

図 5-3　RADIUS アクセス サービス選択規則の追加



小なりボタン（<）を使用すると、割り当てられているデバイス グループの中から選択したものを [Available Device Groups] に戻すことができます。二重大なりボタン（>>）を使用すると、すべての [Available Device Groups] が [Assigned Device Groups] に移動します。二重小なりボタン（<<）を使用すると、すべての [Assigned Device Groups] が [Available Device Groups] に移動します。

[Selection Rules] ウィンドウ（図 5-3）を使用して、事前に定義済みのディクショナリの [RADIUS Request Attributes] 下で [RADIUS attributes] の一覧を表示し、着信 RADIUS アクセス要求に一致する期待値を指定することもできます。

ステップ 6　プルダウン メニューを使用して、ディクショナリを選択します。

次のディクショナリがサポートされています。

- RADIUS IETF
- Cisco IOS
- Cisco VPN 5000
- Microsoft
- ユーザ定義の 4 つのカスタム ディクショナリ

  カスタム ディクショナリは、[System Administration] > [Radius Dictionary] で定義します。

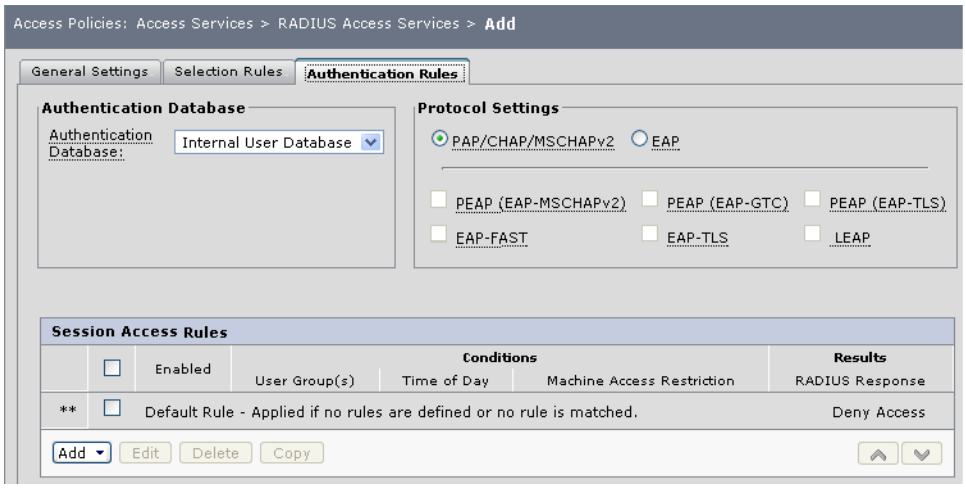
ステップ 7　プルダウン メニューを使用して、選択したディクショナリに固有の RADIUS アトリビュートを選択し、そのアトリビュートに割り当てる値を入力します。

指定したアトリビュートと値（「アトリビュート値のペア」または「AV ペア」とも呼ばれます）は、着信 RADIUS アクセス要求に指定されている必要があります。

ステップ 8　[Results] タブをクリックします。

[Results] タブ ウィンドウ（図 5-4）では、認証データベースの選択、EAP 設定の選択、セッション アクセス規則の定義を行うことができます。

図 5-4　RADIUS アクセス サービス結果の追加



ステップ 9　プルダウン メニューを使用して、認証データベースを選択します。

着信 RADIUS アクセス要求の認証に使用する認証データベースを選択します。

（注）　プルダウン メニューには、設定されたデータベースだけが一覧表示されます。

ステップ 10　このアクセス規則に使用する [Protocol Settings] を選択します。

[Session Access Rules] を使用して、認証されたユーザに付与するエンタイトルメントを決定します。クレデンシャルが有効でない場合、アクセスは拒否され、ACS Express によりネットワーク デバイスに応答が送信されます。

各認証プロトコルと互換性のあるデータベースの一覧については、表 5-1 および「認証プロトコルと互換性のあるデータベース」を参照してください。

表 5-1　認証プロトコルと互換性のあるデータベース

	データベース			
認証プロトコル	**ローカル**	**AD**	**LDAP**	**OTP**
TACACS+（ASCII）	はい	はい	はい	はい
PAP/ASCII	はい	はい	はい	はい
CHAP	はい	いいえ	いいえ	いいえ
MSCHAPv2	はい	はい	いいえ	いいえ
EAP-MSCHAPv2	はい	はい	いいえ	いいえ
LEAP	はい	はい	はい[1]	いいえ
EAP-TLS	はい	はい	はい	いいえ
PEAP（EAP-TLS）	はい	はい	はい	いいえ
PEAP（EAP-GTC）	はい	はい	はい	はい
PEAP（EAP-MSCHAPV2）	はい	はい	いいえ	いいえ
EAP-FASTv0（EAP-GTC）	はい	はい	はい	いいえ
EAP-FASTv0（EAP-MSCHAPv2）	はい	はい	いいえ	いいえ

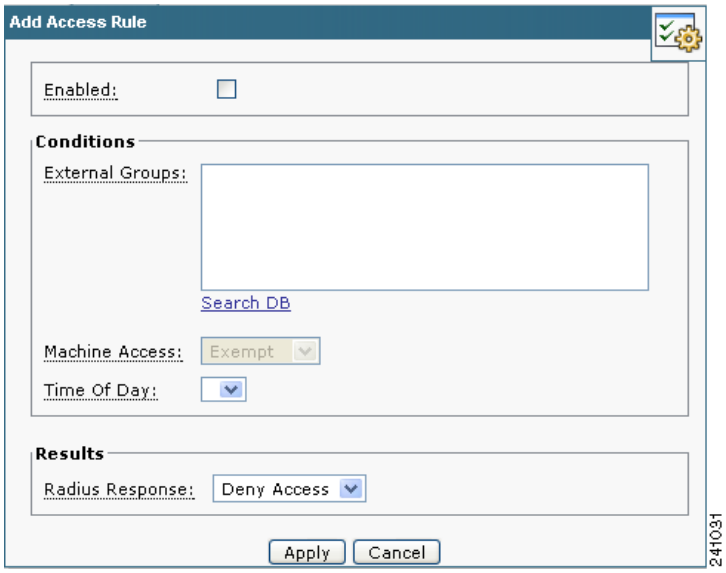
[1] LEAP では、クリア テキストのパスワードが使用されます。

（注）　ACS Express 5.0.1 は、EAP-FASTv1 や EAP-FASTv1a などの最新の EAP-FAST RFC に対して完全準拠ではありません。

ステップ 11　セッション アクセス規則を追加するには、[Add] をクリックし、[Add One] を選択します。

[Add Access Rule] ダイアログ ボックスが表示されます（図 5-5）。

図 5-5　アクセス規則の追加



ステップ 12　[Enabled] チェックボックスをオンにして、アクセス規則を有効にします。

[Selection Rules] 領域で、ユーザ グループを指定し、任意の ToD または マシン アクセス制限を指定します。認証規則に複数のユーザ グループを指定する場合、ユーザは指定したすべてのユーザ グループに属している必要があります。

ステップ 13　[Search DB] をクリックし、このアクセス規則に関連づけるユーザ グループを特定します。

[Search Database Groups] ダイアログが表示されます。

（注）　この動作は、OTP サーバには該当しません。

ステップ 14　[Search Filter] フィールドに完全な名前または部分名（ワイルドカード使用）を入力し、[Search] をクリックします。

（注）　グループ検索では、大文字と小文字が区別されます。アスタリスク（*）ワイルドカードとしてを使用できます。

ステップ 15　検索結果からエントリを選択し、[Apply] をクリックしてグループを選択するか、[Cancel] をクリックして操作を中止します。

ステップ 16　プルダウン メニューを使用して、任意のマシン アクセス制限を選択します。

マシンの認証が成功すると、ACS Express サーバによりマシン セッションが作成され、キャッシュされます。マシン セッションは、MAR タイムアウト時間が経過すると期限が切れます。期限切れとなったセッションは、1 時間ごとにクリーンアップされます。

マシン セッションの期限が切れた後、クリーンアップが行われる前にマシンの再認証が成功すると、新しいセッションは作成されず、既存のセッションが使用されます。セッションの期限が切れ、MAR によってアクセス規則が強制されたマシンでユーザ認証が行われた場合、ユーザ認証は拒否されます。

ステップ 17　プルダウン メニューを使用して、時間帯のブロックを選択します。

このフィールドはオプションです。選択しないと、ToD は無視されます。

ステップ 18　プルダウン メニューを使用して、RADIUS 応答を選択します。

ステップ 19　この RADIUS アクセス サービスを保存する場合は [Apply] をクリックします。中止する場合は [Cancel] をクリックします。

RADIUS アクセス サービスの編集

RADIUS アクセス サービスを編集するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [RADIUS Access Services] を選択します。

[Access Policies: Access Services] > [RADIUS Access Services] ウィンドウに、現在定義されている RADIUS アクセス サービスが表示されます。

ステップ 2　対応するチェックボックスをオンにして変更する RADIUS アクセス サービスを選択し、[Edit] > [Edit Status]、[Edit Selection Rules]、または [Edit Results] をクリックします。

選択したタブに応じて、[Edit] ダイアログ ボックスが表示されます。その他のタブをクリックして、該当する領域で変更を加えることもできます。

ステップ 3　アクセス サービスに対し、必要な変更を行います。

ステップ 4　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

RADIUS アクセス サービスのコピー

RADIUS アクセス サービスをコピーするには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [RADIUS Access Services] を選択します。

[Access Policies: Access Services] > [RADIUS Access Services] ウィンドウに、現在定義されている RADIUS アクセス サービスが表示されます。

ステップ 2　対応するチェックボックスをオンにしてコピーする RADIUS アクセス サービスを選択し、[Copy] をクリックします。

選択した RADIUS アクセス サービスの [Copy] ダイアログ ボックスが表示されます。アクセス サービスの名前が、[Copy-of-*access_service*] として一覧表示されます。

ステップ 3　アクセス サービスの名前を変更し、コピーしたアクセス サービスに必要な変更を加えます。

ステップ 4　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

RADIUS アクセス サービスの削除

RADIUS アクセス サービスを削除するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [RADIUS Access Services] を選択します。

[Access Policies: Access Services] > [RADIUS Access Services] ウィンドウに、現在定義されている RADIUS アクセス サービスが表示されます。

ステップ 2　対応するチェックボックスをオンにして削除する RADIUS アクセス サービスを選択し、[Delete] をクリックします。

[Confirm Deletion] ダイアログ ボックスが開き、選択したアクセス サービスを削除してよいかどうかを確認するメッセージが表示されます。

ステップ 3　選択した RADIUS アクセス サービスを削除する場合は [Yes] をクリックします。中止して RADIUS アクセス サービスの一覧に戻る場合は [No] をクリックします。

TACACS+ アクセス サービス

ここでは、TACACS+ アクセス サービスを管理する方法について説明します。ACS Express では、1 つの TACACS+ アクセス サービスだけをサポートしています。TACACS+ アクセス サービスを使用するには、使用するユーザ データベース、タイムアウト設定、およびアクセス規則を設定します。ユーザ データベースとタイムアウト設定は、すべての TACACS+ アクセス規則に共通です。

TACACS+ アクセス サービスを使用するには、TACACS+ 共有秘密情報のあるデバイスを設定し、アクセスを許可する TACACS+ アクセス サービスのアクセス規則を設定する必要があります。

この項は、次の内容で構成されています。

- 「1 つの TACACS+ アクセス サービスのアクセス規則の追加」（P.5-9）
- 「複数の TACACS+ アクセス規則の追加」（P.5-10）
- 「TACACS+ アクセス規則の編集」（P.5-11）
- 「TACACS+ アクセス規則のコピー」（P.5-11）

- 「TACACS+ アクセス規則の削除」（P.5-12）

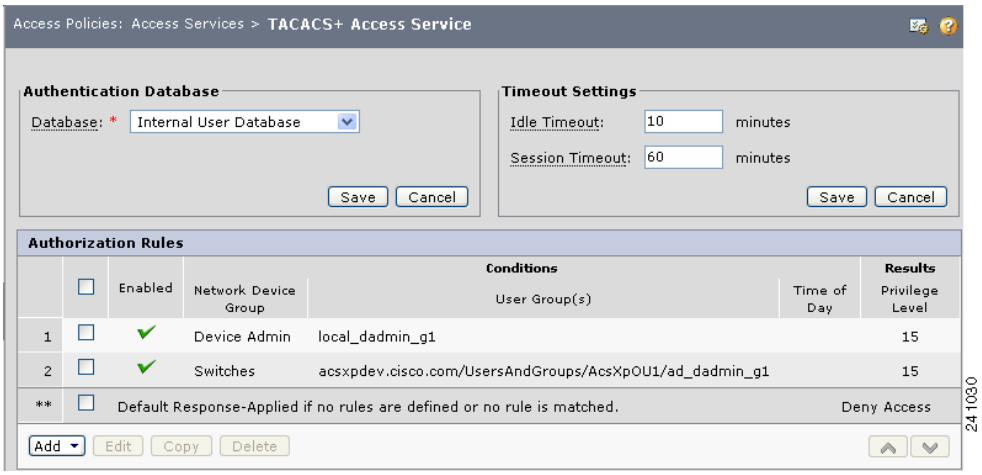
1 つの TACACS+ アクセス サービスのアクセス規則の追加

1 つの TACACS+ アクセス サービスのアクセス規則を追加するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [TACACS+ Access Services] を選択します。

[Access Policies: Access Services] > [TACACS+ Access Services] ウィンドウに、現在定義されているすべての TACACS+ アクセス サービスが表示されます（図 5-6 を参照）。

図 5-6　TACACS+ アクセス サービスの追加



ステップ 2　[Add] > [Add One] をクリックします。

[Add Access Rule] ダイアログ ボックスが表示されます。新しいアクセス規則のデフォルトのステータスは [Enabled] です。

ステップ 3　[Status] を [Enabled] のまま受け入れるか、プルダウン メニューを使用して [Disabled] に変更します。

ステップ 4　プルダウン メニューを使用して、いずれかのネットワーク デバイス グループを選択します。

ステップ 5　[Search DB] をクリックし、このアクセス規則に関連付ける [User Group] を選択します。

[Search Database Groups] ダイアログ ボックスが表示されます。

（注）　この動作は、OTP サーバには該当しません。

ステップ 6　[Search Filter] フィールドに完全な名前または部分名（ワイルドカード使用）を入力し、[Search] をクリックします。

（注）　検索では、大文字と小文字が区別されます。アスタリスク（*）ワイルドカードとしてを使用できます。

ステップ 7　検索結果からエントリを選択し、[Apply] をクリックしてユーザ グループを選択するか、[Cancel] をクリックして操作を中止します。

ステップ 8　前に設定したいずれかの ToD ブロックを選択します。

ToD ブロックは、アクセスが許可される時間帯（曜日と時間）を示すものです。このフィールドはオプションです。選択しないと、ToD は無視されます。

このアクセス規則を使用してアクセスを許可するには、[Results] の下にある [Deny Access] チェックボックスをオフにします。[Deny Access] チェックボックスをオフにしてアクセスを許可する場合、特権レベルを選択する必要があります。

ステップ 9　プルダウン メニューを使用して、アクセス規則の特権レベル（0 ～ 15）を選択します。

ステップ 10　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

複数の TACACS+ アクセス規則の追加

複数の TACACS+ アクセス規則を追加するには、次の手順を実行します。

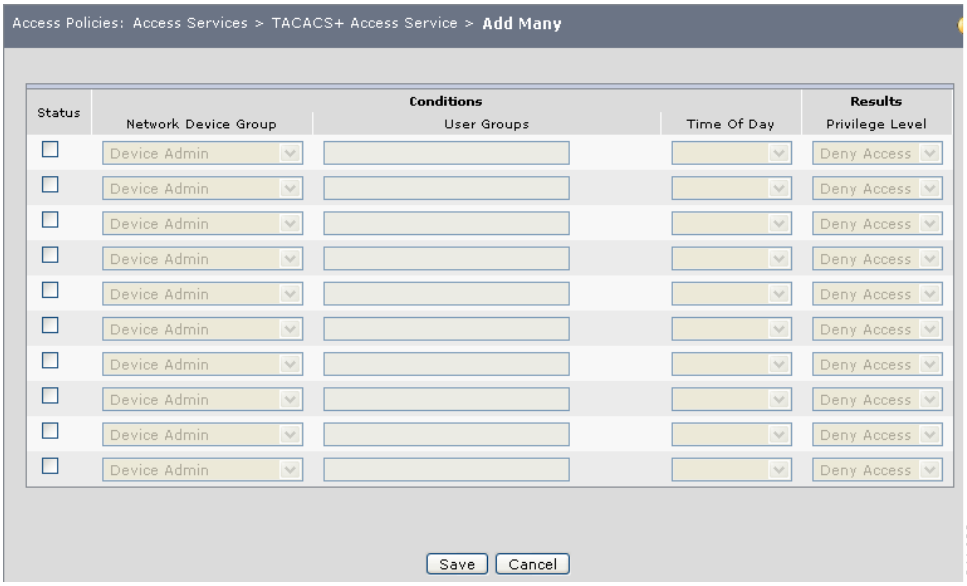
ステップ 1　[Access Policies] を選択し、[Access Services] 下の [TACACS+ Access Services] を選択します。

[Access Policies: Access Services] > [TACACS+ Access Services] ウィンドウに、現在定義されている TACACS+ アクセス サービスが表示されます。

ステップ 2　[Add] > [Add Many] をクリックします。

[Add Many] ダイアログ ボックス（図 5-7）が表示されます。新しいアクセス規則のデフォルトのステータスは [Enabled] です。

図 5-7　複数の TACACS+ 認可規則の追加



ステップ 3　[Status] チェックボックスをオンにして、追加する各アクセス規則のプロパティを入力します。

[Status] チェックボックスをオンにすると、その行にあるフィールドとプルダウン メニューがアクティブになります。

ステップ 4　プルダウン メニューを使用して、ネットワーク デバイス グループを選択します。

ステップ 5　各アクセス規則に関連付けるユーザ グループを入力します。

ステップ 6　各アクセス規則に使用する ToD ブロックを選択します。

このフィールドはオプションです。選択しないと、ToD は無視されます。

ステップ 7　アクセスを許可するには、プルダウン メニューを使用して、各アクセス規則の特権レベルを選択します。

ステップ 8　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

TACACS+ アクセス規則の編集

TACACS+ アクセス規則を編集するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [TACACS+ Access Services] を選択します。

[Access Policies: Access Services] > [TACACS+ Access Services] ウィンドウに、現在定義されている TACACS+ アクセス サービスが表示されます。

ステップ 2　対応するチェックボックスをオンにして変更するアクセス規則を選択し、[Edit] をクリックします。

[TACACS+ Access Service] > [Edit Access Rule] ウィンドウが表示されます。

ステップ 3　必要な変更を加え、保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

複数の TACACS+ アクセス規則の編集

ACS Express では、既に設定した TACACS+ アクセス規則について、同時に複数のプロパティを変更できます。

複数の TACACS+ アクセス規則を編集するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [TACACS+ Access Services] を選択します。

[Access Policies: Access Services] > [TACACS+ Access Services] ウィンドウに、現在定義されている TACACS+ アクセス サービスが表示されます。

ステップ 2　変更する各 TACACS+ アクセス規則のチェックボックスをオンにして、[Edit] をクリックします。

[TACACS+ Access Service] > [Edit Many] ウィンドウが表示されます。ACS Express GUI にも、編集するように選択した規則と、各プロパティに現在設定されている値が表示されます。

ステップ 3　TACACS+ アクセス規則で変更または追加する各プロパティのチェックボックスをオンにします。

追加または変更するプロパティを選択すると、関連付けられたフィールドがアクティブになり、値を追加または変更できるようになります。

ステップ 4　必要な変更をすべて加えた後、変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

TACACS+ アクセス規則のコピー

TACACS+ アクセス規則をコピーするには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [TACACS+ Access Services] を選択します。

[Access Policies: Access Services] > [TACACS+ Access Services] ウィンドウに、現在定義されている TACACS+ アクセス サービスが表示されます。

ステップ 2　対応するチェックボックスをオンにしてコピーするアクセス規則を選択し、[Copy] をクリックします。

[TACACS+ Access Service] > [Edit Access Rule] ウィンドウが表示されます。

ステップ 3　必要な変更を加え、保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

TACACS+ アクセス規則の削除

TACACS+ アクセス規則を削除するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Access Services] 下の [TACACS+ Access Services] を選択します。

[Access Policies: Access Services] > [TACACS+ Access Services] ウィンドウに、現在定義されている TACACS+ アクセス サービスが表示されます。

ステップ 2　対応するチェックボックスをオンにして削除するアクセス規則を選択し、[Delete] をクリックします。

[Confirm Deletion] ダイアログ ボックスが開き、アクセス規則を削除してよいかどうかを確認するメッセージが表示されます。

ステップ 3　選択したアクセス規則を削除するには [Yes] をクリックします。操作を中止して規則を保持するには [No] をクリックします。

ポリシー要素

次のポリシー要素を設定するには、ACS Express GUI を使用します。

- 「RADIUS 応答」（P.5-12）
- 「時間帯」（P.5-14）

RADIUS 応答

RADIUS 応答を使用して、環境ディクショナリの集合から RADIUS アトリビュートの値のペアのセットを定義できます。ACS Express では、次のディクショナリのアトリビュートをサポートしています。

- RADIUS - IETF
- Cisco Airespace
- Cisco IOS
- Cisco VPN 3000 ASA PIX 7.+
- Cisco VPN 5000
- 4 つのカスタム ディクショナリ
- Juniper
- Microsoft

RADIUS 応答の追加

ACS Express では、最大 10 のアトリビュート/値（AV）ペアを使用して、RADIUS 応答セット（または RADIUS アトリビュート セット）を設定できます。

RADIUS 応答（または RADIUS アトリビュート セット）を追加するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [RADIUS Response] を選択します。

[Access Policies] > [Policy Elements] > [RADIUS Response] ウィンドウに、現在定義されている RADIUS アトリビュート セットが表示されます。

ステップ 2　新しい RADIUS アトリビュート セットを設定するには、[Access Policies] > [Policy Elements] > [RADIUS Response] を選択し、[Add] をクリックします。

[Add] ウィンドウが表示されます。

ステップ 3　新しいアトリビュート セットの名前を入力します。

ステップ 4　（オプションで）アトリビュート セットの説明を入力します。

ステップ 5　ドロップダウン メニューから、使用するアトリビュートが含まれるディクショナリを選択します。

ステップ 6　[Attribute] リストで、使用するアトリビュートを選択します。

ステップ 7　[Tag] フィールドに、アトリビュートの値を入力します。

RADIUS 応答の AV ペアを必要なだけ入力します（最大 10 個）。

ステップ 8　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

RADIUS 応答の編集

RADIUS 応答（または RADIUS アトリビュート セット）を編集するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [RADIUS Response] を選択します。

[Access Policies] > [Policy Elements] > [RADIUS Response] ウィンドウに、現在定義されている RADIUS アトリビュート セットが表示されます。

ステップ 2　RADIUS アトリビュート セットを編集するには、対応するチェックボックスをオンにして RADIUS アトリビュート セットを選択するか、既存のアトリビュート セットの名前をクリックします。

[Access Policies] > [Policy Elements] > [RADIUS Response] > [Edit] ウィンドウが表示されます。

ステップ 3　アトリビュート セットに必要な変更を加えます。

ステップ 4　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

RADIUS 応答のコピー

RADIUS 応答（または RADIUS アトリビュート セット）をコピーするには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [RADIUS Response] を選択します。

[Access Policies] > [Policy Elements] > [RADIUS Response] ウィンドウに、現在定義されている RADIUS アトリビュート セットが表示されます。

ステップ 2　RADIUS アトリビュート セットをコピーするには、対応するチェックボックスをオンにして RADIUS アトリビュート セットを選択するか、既存のアトリビュート セットの名前をクリックします。

[Access Policies] > [Policy Elements] > [RADIUS Response] > [Edit] ウィンドウが表示されます。

ステップ 3　RADIUS 応答の名前を変更し、アトリビュート セットにその他の必要な変更を加えます。

ステップ 4　変更を保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

RADIUS 応答の削除

RADIUS 応答（または RADIUS アトリビュート セット）を削除するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [RADIUS Response] を選択します。

[Access Policies] > [Policy Elements] > [RADIUS Response] ウィンドウに、現在定義されている RADIUS アトリビュート セットが表示されます。

ステップ 2　RADIUS アトリビュート セットを削除するには、対応するチェックボックスをオンにし、[Delete] をクリックします。

ダイアログ ボックスで、選択した RADIUS アトリビュート セットは完全に削除されることが通知されます。

ステップ 3　選択したアトリビュート セットを削除する場合は [OK] をクリックします。中止する場合は [Cancel] をクリックします。

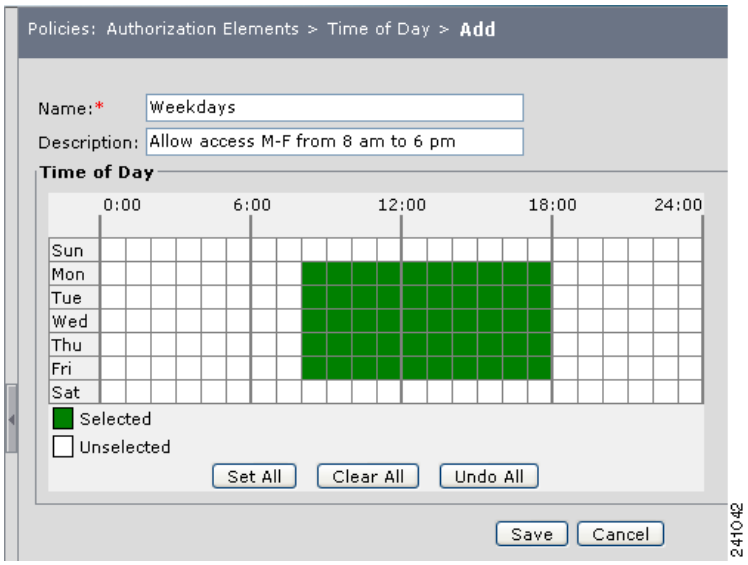
時間帯

[ToD] ウィンドウでは、任意の曜日（複数可）を対象に、アクセスを許可する時間帯を選択できます。たとえば、平日、午後、夜の交代勤務時間を定義し、それぞれの所定の就労時間にのみユーザ アクセスを許可するようにできます。図 5-8 は、平日の交代勤務時間（午前 8:00 ～午後 6:00（0800 ～ 1800）、月曜～金曜）を定義する時間ブロックの例を示したものです。

ここでは、次の内容について説明します。

- 「時間帯ブロックの追加」（P.5-15）
- 「時間帯ブロックの編集」（P.5-15）
- 「時間帯ブロックのコピー」（P.5-16）
- 「時間帯ブロックの削除」（P.5-17）

図 5-8　時間帯ブロック



時間帯ブロックの追加

ToD を追加するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [Time of Day] を選択します。

[Access Policies] > [Policy Elements] > [Time of Day] ウィンドウに、現在定義されている ToD ブロックの一覧が表示されます。

ステップ 2　新しい ToD ブロックを定義するには、[Add] をクリックします。

[Access Policies] > [Policy Elements] > [Time of Day] > [Add] ウィンドウに、7 日間、24 時間のグリッドが表示されます。

ステップ 3　この ToD ブロックの名前を入力します。

この名前は、ユーザ グループを設定するときのメニュー項目選択に使用されます。

ステップ 4　（オプションで）この ToD ブロックの説明を入力することもできます。

ステップ 5　マウスを使用して、グリッドで、この ToD ブロックでアクセス可能とする時間を選択します。

グリッドで特定の時間をクリックするか、または時間の複数の行を同時に選択できます。時間の行を選択するには、最初の時間を左クリックし、**Shift** キーを押しながら最後の時間までドラッグします。引き続き、**Shift** キーを押しながらグリッド内の追加の時間や行を選択できます。

ステップ 6　ToD ブロックを保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

時間帯ブロックの編集

ToD ブロックを編集するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [Time of Day] を選択します。

[Access Policies] > [Policy Elements] > [Time of Day] ウィンドウに、現在定義されている ToD ブロックの一覧が表示されます。

ステップ 2　ToD ブロックを編集するには、対応するチェックボックスをオンにして ToD ブロックを選択するか、または既存の ToD ブロックの名前をクリックして [Edit] をクリックします。

[Access Policies] > [Policy Elements] > [Time of Day] > [Add] ウィンドウに、7 日間、24 時間のグリッドが表示されます。

ステップ 3　この ToD ブロックで必要なすべての変更を加えます。

この名前は、ユーザ グループを設定するときのメニュー項目選択に使用されます。

ステップ 4　（オプションで）この ToD ブロックの説明を入力することもできます。

ステップ 5　マウスを使用して、グリッドで、この ToD ブロックでアクセス可能とする時間を選択します。

グリッドで特定の時間をクリックするか、または時間の複数の行を同時に選択できます。時間の行を選択するには、最初の時間を左クリックし、**Shift** キーを押しながら最後の時間までドラッグします。引き続き、**Shift** キーを押しながらグリッド内の追加の時間や行を選択できます。

ステップ 6　ToD ブロックを保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

時間帯ブロックのコピー

ToD をコピーするには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [Time of Day] を選択します。

[Access Policies] > [Policy Elements] > [Time of Day] ウィンドウに、現在定義されている ToD ブロックの一覧が表示されます。

ステップ 2　ToD ブロックをコピーするには、対応するチェックボックスをオンにするか、または既存の ToD ブロックの名前をクリックして [Copy] をクリックします。

[Access Policies] > [Policy Elements] > [Time of Day] > [Copy] ウィンドウに、7 日間、24 時間のグリッドが表示されます。

ステップ 3　新しい ToD ブロックの名前を入力します。

この名前は、ユーザ グループを設定するときのメニュー項目選択に使用されます。

ステップ 4　（オプションで）この ToD ブロックの説明を入力することもできます。

ステップ 5　マウスを使用して、この ToD ブロックで必要な変更を加えます。

グリッドで特定の時間をクリックするか、または時間の複数の行を同時に選択できます。時間の行を選択するには、最初の時間を左クリックし、**Shift** キーを押しながら最後の時間までドラッグします。引き続き、**Shift** キーを押しながらグリッド内の追加の時間や行を選択できます。

ステップ 6　ToD ブロックを保存する場合は [Save] をクリックします。中止する場合は [Cancel] をクリックします。

時間帯ブロックの削除

ToD ブロックを削除するには、次の手順を実行します。

ステップ 1　[Access Policies] を選択し、[Policy Elements] 下の [Time of Day] を選択します。

[Access Policies] > [Policy Elements] > [Time of Day] ウィンドウに、現在定義されている ToD ブロックの一覧が表示されます。

ステップ 2　ToD ブロックを削除するには、削除する ToD ブロックのチェックボックスをオンにして、[Delete] をクリックします。

ダイアログ ボックスが開き、ToD ブロックを削除してよいかどうかを確認するメッセージが表示されます。

ステップ 3　ToD ブロックを削除する場合は [OK] をクリックします。中止する場合は [Cancel] をクリックします。