CHAPTER 18

システム管理設定の管理

Cisco Secure ACS をインストールしたあとに、ネットワークを効率的に管理するように ACS を設定および管理する必要があります。ACS Web インターフェイスを使用すると、ACS を簡単に設定してさまざまな処理を実行できます。ACS の使用を開始するために必要なインストール後の設定作業のリストについては、第 6 章「インストール後の設定タスク」を参照してください。

[System Administration] > [Configuration] を選択すると、次の操作を実行できるページにアクセスできます。

- TACACS+、EAP-TLS、PEAP、EAP-FAST の設定など、グローバル システム オプションの設定。「グローバル システム オプションの設定」（P.18-1）を参照してください。
- プロトコル ディクショナリの設定。「ディクショナリの管理」（P.18-5）を参照してください。
- ローカル サーバ証明書の管理。「ローカル サーバ証明書の設定」（P.18-14）を参照してください。
- ログ設定の管理。「ログの設定」（P.18-21）を参照してください。
- ライセンスの管理。「ライセンスの概要」（P.18-35）を参照してください。

グローバル システム オプションの設定

[System Administration] > [Configuration] > [Global System Options] の各ページに、次のオプションがあります。

- 「TACACS+ の設定」（P.18-1）
- 「EAP-TLS の設定」（P.18-2）
- 「PEAP の設定」（P.18-3）
- EAP-FAST の設定
- EAP-FAST PAC の生成

TACACS+ の設定

[TACACS+ Settings] ページは、TACACS+ の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [TACACS+ Settings] を選択します。

表 18-1 で説明されている [TACACS+ Settings] ページが表示されます。

表 18-1　TACACS+ Settings

オプション	説明
Port to Listen	リッスンするポート番号。
Connection Timeout	接続がタイムアウトするまでの分数。
Session Timeout	セッションがタイムアウトするまでの分数。
Maximum Packet Size	最大パケット サイズ（バイト単位）。
Single Connect Support	単一接続のサポートをイネーブルにする場合にオンにします。
Login Prompts	
Username Prompt	ユーザ名プロンプトとして使用するテキスト文字列。
Password Prompt	パスワード プロンプトとして使用するテキスト文字列。
Password Change Control	
Enable TELNET Change Password	TELNET セッション中にパスワードを変更するオプションを指定する場合に選択します。
Prompt for Old Password:	古いパスワードのプロンプトとして使用するテキスト文字列。
Prompt for New Password	新しいパスワードのプロンプトとして使用するテキスト文字列。
Prompt for Confirm Password	パスワードの確認プロンプトとして使用するテキスト文字列。
Disable TELNET Change Password	TELNET セッション中にパスワードを変更しない場合に選択します。
Message when Disabled	[Disable TELNET Change Password] オプションを選択した場合に表示されるメッセージ。

EAP-TLS の設定

[EAP-TLS Settings] ページは、EAP-TLS の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [EAP-TLS Settings] を選択します。

表 18-2 で説明されている [EAP-TLS Settings] ページが表示されます。

表 18-2　EAP-TLS Settings

オプション	説明
General	
Enable EAP-TLS Session Resume	完全な EAP-TLS 認証に成功したユーザの簡略化された再認証をサポートする場合にオンにします。 この機能を使用すると、証明書を使用しないで SSL ハンドシェイクだけでユーザの再認証が行われます。EAP-TLS セッション再開機能は、指定された EAP-TLS セッション タイムアウト値以内でだけ動作します。
EAP-TLS Session Timeout	EAP-TLS セッションがタイムアウトするまでの秒数を入力します。デフォルト値は 7200 秒です。
Stateless Session Resume	

表 18-2　EAP-TLS Settings （続き）

オプション	説明
Master Key Generation Period	値が指定された期間後にマスター キーの再生成に使用されます。デフォルトは 1 週間です。
Revoke	以前のマスター キーをすべてキャンセルするには、[Revoke] をクリックします。この処理を使用する場合は注意が必要です。 ACS ノードがセカンダリ ノードの場合、[Revoke] オプションはディセーブルになります。

PEAP の設定

[PEAP Settings] ページは、PEAP の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [PEAP Settings] を選択します。

表 18-3 で説明されている [PEAP Settings] ページが表示されます。

表 18-3　PEAP Settings

オプション	説明
Enable PEAP Session Resume	オンにすると、ACS は、ユーザが PEAP 認証のフェーズ 2 で正常に認証された場合にかぎり、PEAP 認証のフェーズ 1 で作成された TLS セッションをキャッシュします。ユーザが再接続しようとする場合、元の PEAP セッションがタイムアウトしていなければ、ACS はキャッシュされた TLS セッションを使用します。このため、PEAP のパフォーマンスが向上し、AAA サーバの負荷が軽減されます。 PEAP セッション再開機能を動作させるには、PEAP セッション タイムアウト値を指定する必要があります。
PEAP Session Timeout	PEAP セッションがタイムアウトするまでの秒数を入力します。デフォルト値は 7200 秒です。
Enable Fast Reconnect	セッション再開機能がイネーブルの場合に、PEAP セッションがユーザ クレデンシャルを確認しないで ACS で再開することを許可する場合にオンにします。

関連項目

- 「EAP-FAST PAC の生成」（P.18-4）

EAP-FAST の設定

[EAP-FAST Settings] ページは、EAP-FAST の実行時の特性を設定する場合に使用します。

[System Administration] > [Configuration] > [Global System Options] > [EAP-FAST] > [Settings] を選択します。

表 18-4 で説明されている [EAP-FAST Settings] ページが表示されます。

表 18-4　EAP-FAST Settings

オプション	説明
General	
Authority Identity Info Description	クレデンシャルをクライアントに送信する ACS サーバを説明したわかりやすい文字列。クライアントは、この文字列を Protected Access Credentials Information（PAC-Info）Type-Length-Value（TLV）で認識できます。デフォルト値は [Cisco Secure ACS] です。
Master Key Generation Period	この値は、PAC の暗号化や復号化および署名や認証に使用されます。デフォルトは 1 週間です。
Revoke	
Revoke	以前のマスターキーと PAC をすべて無効にするには、[Revoke] をクリックします。この処理を使用する場合は注意が必要です。 ACS ノードがセカンダリ ノードの場合、[Revoke] オプションはディセーブルになります。

EAP-FAST PAC の生成

EAP-FAST の [Generate PAC] ページは、ユーザ PAC またはマシン PAC を生成する場合に使用します。

ステップ 1　[System Administration] > [Configuration] > [Global System Options] > [EAP-FAST] > [Generate PAC] を選択します。

表 18-5 で説明されている [Generate PAC] ページが表示されます。

表 18-5　Generate PAC

オプション	説明
Tunnel PAC	トンネル PAC を生成する場合に選択します。
Machine PAC	マシン PAC を生成する場合に選択します。
Identity	EAP-FAST プロトコルによって「内部ユーザ名」として提示されたユーザ名またはマシン名を指定します。ID 文字列がそのユーザ名と一致しない場合、認証は失敗します。
PAC Time To Live	秒、分、時間、日、週、月、および年に対応する最大値を入力します。正の整数を入力してください。
Password	パスワードを入力します。

ステップ 2　[Generate PAC] をクリックします。

RSA SecurID プロンプトの設定

ACS 展開用の RSA プロンプトを設定できます。設定した RSA プロンプトのセットは、構成内のすべての RSA 領域と ACS インスタンスに使用されます。RSA SecurID プロンプトを設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Global System Options] > [RSA SecurID Prompts] を選択します。

[RSA SecurID Prompts] ページが表示されます。

ステップ 2　表 18-6 で説明されているフィールドを変更します。

表 18-6　[RSA SecurID Prompts] ページ

オプション	説明
Passcode Prompt	パスコードを要求するテキスト文字列。デフォルト値は [Enter PASSCODE:] です。
Next Token Prompt	次のトークンを要求するテキスト文字列。デフォルト値は [Enter Next TOKENCODE:] です。
Choose PIN Type Prompt	PIN タイプを要求するテキスト文字列。デフォルト値は [Do you want to enter your own pin?] です。
Accept System PIN Prompt	システム生成の PIN を受け付けるテキスト文字列。デフォルト値は [ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?] です。
次に示す 2 つの PIN 入力プロンプトでは、プロンプトに次の文字列が含まれている場合、次のように置き換えられます。 • {MIN_LENGTH}：RSA 領域に設定されている最小 PIN 長に置き換えられます。 • {MAX_LENGTH}：RSA 領域に設定されている最大 PIN 長に置き換えられます。 • /x/：新しい PIN 手順をキャンセルする。	
Alphanumeric PIN Prompt	英数字の PIN を要求するテキスト文字列。
Numeric PIN Prompt	数値の PIN を要求するテキスト文字列。
Re-Enter PIN Prompt	ユーザに PIN の再入力を要求するテキスト文字列。デフォルト値は [Reenter PIN:] です。

ステップ 3　[Submit] をクリックして RSA SecurID プロンプトを保存します。

ディクショナリの管理

[System Administration] > [Configuration] > [Dictionaries] を選択すると、次のタスクを実行できます。

- 「RADIUS 属性と TACACS+ 属性の表示」（P.18-5）
- 「ID ディクショナリの設定」（P.18-10）

RADIUS 属性と TACACS+ 属性の表示

RADIUS と TACACS+ の [Dictionary] ページには、次のディクショナリ内の使用可能なプロトコル属性が表示されます。

- RADIUS（IETF）
- RADIUS（Cisco）
- RADIUS（Microsoft）

- RADIUS（Ascend）
- RADIUS（Cisco Airespace）
- RADIUS（Cisco Aironet）
- RADIUS（Cisco BBSM）
- RADIUS（Cisco VPN 3000）
- RADIUS（Cisco VPN 5000）
- RADIUS（Juniper）
- RADIUS（Nortel [Bay Networks]）
- RADIUS（RedCreek）
- RADIUS（US Robotics）
- TACACS+

プロトコル ディクショナリの属性を表示および選択するには、[System Administration] > [Configuration] > [Dictionaries] > [Protocols] を選択してからディクショナリを選択します。

表 18-7 で説明されている使用可能な属性のリストを含む [Dictionary] ページが表示されます。

表 18-7　プロトコルの [Dictionary] ページ

オプション	説明
Attribute	属性の名前
ID	（RADIUS のみ）VSA ID。
Type	属性のデータ型。
Direction	（RADIUS のみ）属性の使用場所として、要求内、応答内、またはその両方を指定します。単一または双方向認証。
Multiple Allowed	（RADIUS のみ）複数の属性を許可します。*multiple allowed* を指定する属性は、1 つの要求または応答で複数回使用可能です。

属性のリストをスクロールするには、矢印を使用します。

ACS 5.4 では、RADIUS ベンダー固有属性（VSA）もサポートされています。事前定義済みの RADIUS VSA のセットを使用できます。ACS Web インターフェイスで追加のベンダーと属性を定義できます。RADIUS VSA は作成、編集、または削除できます。

新しく定義した VSA は、事前定義済みの VSA と同様にポリシー、認可プロファイル、および RADIUS トークン サーバで使用できます。詳細については、以下を参照してください。

- 「RADIUS VSA」（P.A-6）。
- 「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）

RADIUS ベンダー固有属性の作成、複製、および編集

ベンダー固有属性（VSA）を使用すると、ベンダーは RADIUS 属性の機能拡張を作成できます。ベンダーには固有のベンダー番号が割り当てられています。VSA は、サブ属性が含まれる属性です。ACS 5.4 では、RADIUS VSA を作成、複製、または編集できます。次の手順を実行します。

内部で使用される属性の一部は変更できません。

属性がポリシーまたはポリシー要素によって使用されている場合は、属性のタイプを変更できません。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS VSA] を選択します。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する RADIUS VSA の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 編集する RADIUS VSA の隣にあるチェックボックスをオンにし、[Edit] をクリックします。

[Create RADIUS VSA] ページが表示されます。表 18-8 で説明されているフィールドを変更します。

表 18-8　RADIUS VSA：作成、複製、編集ページ

オプション	説明
Attribute	RADIUS VSA の名前。
Description	（任意）RADIUS VSA の簡単な説明。
Vendor ID	RADIUS ベンダーの ID。
Attribute Prefix	（任意）ベンダーのすべての属性が同じプレフィックスで始まるように、RADIUS 属性にプリペンドするプレフィックス。
Use Advanced Vendor Options	
Vendor Length Field Size	VSA の長さを指定するための 8 ビットのベンダー長フィールド。VSA のベンダー長を選択します。有効なオプションは 0 と 1 です。デフォルト値は、1 です
Vendor Type Field Size	8 ビットのベンダー タイプ フィールド。VSA のベンダー タイプを選択します。有効なオプションは 1、2、および 4 です。デフォルト値は、1 です

ステップ 3　[Submit] をクリックして変更を保存します。

関連トピック

「RADIUS 属性と TACACS+ 属性の表示」（P.18-5）

RADIUS ベンダー固有サブ属性の作成、複製、および編集

RADIUS ベンダー固有サブ属性を作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS] > [RADIUS VSA] を選択します。

または、ナビゲーション ペインから [RADIUS VSA] を選択することもできます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックして、この RADIUS VSA のサブ属性を作成します。
- 複製する RADIUS VSA の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。

- 編集する RADIUS VSA の隣にあるチェックボックスをオンにし、[Edit] をクリックします。

RADIUS VSA サブ属性の作成ページが表示されます。

ステップ 3　表 18-9 で説明されているフィールドに入力します。

表 18-9　RADIUS サブ属性の作成、複製、および編集

オプション	説明
General	
Attribute	サブ属性の名前。名前は一意である必要があります。
Description	（任意）サブ属性の簡単な説明。
RADIUS Configuration	
Vendor Attribute ID	サブ属性のベンダー ID フィールドを入力します。この値は、このベンダーに固有である必要があります。
Direction	属性の使用場所として、要求内、応答内、またはその両方を指定します。単一または双方向認証。
Multiple Allowed	複数の属性を許可します。*multiple allowed* を指定する属性は、1 つの要求または応答で複数回使用可能です。
Include attribute in the log	サブ属性をログに含める場合にオンにします。慎重に扱う必要がある属性の場合は、このチェックボックスをオフにして、属性がロギングされないようにすることができます。
Attribute Type	
Attribute Type	属性のタイプ。有効なオプションは次のとおりです。 • String • Unsigned Integer 32 • IPv4 Address • HEX String • [Enumeration]：このオプションを選択した場合は、ID-Value ペアを入力する必要があります。 ポリシー条件では、HEX String タイプの属性を使用できません。

表 18-9　RADIUS サブ属性の作成、複製、および編集 （続き）

オプション	説明
ID-Value	（任意）*Enumeration 属性タイプの場合のみ。* • [ID] : 0 ～ 999 の数字を入力します。 • [Value] : ID の値を入力します。 • [Add] をクリックして、この ID-Value ペアを ID-Value テーブルに追加します。 ID-Value ペアを編集、置換、および削除するには、次の手順を実行します。 • ID-Value テーブルから ID-Value ペアを選択します。 • [ID] および [Value] フィールドを編集するには、[Edit] をクリックします。必要に応じてフィールドを編集します • フィールドを変更したあとで新しいエントリを追加するには、[Add] をクリックします。 • 同じエントリを異なる値で置換するには、[Replace] をクリックします。 • ID-Value テーブルからエントリを削除するには、[Delete] をクリックします。
Attribute Configuration	
Add Policy Condition	このサブ属性を使用するポリシー条件を入力する場合にオンにします。
Policy Condition Display Name	このサブ属性を使用するポリシー条件の名前を入力します。

ステップ 4　[Submit] をクリックしてサブ属性を保存します。

RADIUS ベンダー固有サブ属性の表示

特定の RADIUS ベンダーでサポートされている属性を表示するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS] > [RADIUS VSA] を選択します。

[RADIUS VSA] ページが表示されます。

ステップ 2　属性を表示するベンダーの隣にあるチェックボックスをオンにし、[Show Vendor Attributes] をクリックします。

ベンダー固有属性および表 18-7 に示されているフィールドが表示されます。追加の VSA を作成したり、これらの属性を複製または編集したりできます。詳細については、「RADIUS ベンダー固有サブ属性の作成、複製、および編集」（P.18-7）を参照してください。

関連項目

「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）

ID ディクショナリの設定

ここでは、次の内容について説明します。

内部ユーザ ID 属性の作成、複製、および編集

内部ユーザ ID 属性を作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択します。

[Internal Users] ページに [Attributes] リストが表示されます。

ステップ 2　次のアクションのいずれかを実行します。

- [Create] をクリックします。
- 複製する属性の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する属性名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

[Identity Attribute Properties] ページが表示されます。

ステップ 3　必要に応じて、[Identity Attributes Properties] ページのフィールドを変更します。フィールドの説明については、「内部 ID 属性の設定」（P.18-11）を参照してください。

ステップ 4　[Submit] をクリックします。

内部ユーザ属性の設定が保存されます。[Internal Users] ページの [Attributes] リストが新しい属性設定で表示されます。

関連トピック

- 「内部ユーザ ID 属性の削除」（P.18-12）
- 「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）
- 「ポリシーおよび ID 属性」（P.3-17）

内部 ID 属性の設定

表 18-10 に、内部 <*users* | *hosts*> ID 属性のフィールドを示します。

表 18-10　[Identity Attribute Properties] ページ

オプション	説明
General	
Attribute	属性の名前
Description	属性の説明。
Attribute Type	
Attribute Type	（任意）ドロップダウン リスト ボックスを使用して、属性タイプを選択します。有効なオプションは次のとおりです。 • String：ページの [Maximum Length] フィールドと [Default Value] フィールドにデータが読み込まれます。属性タイプとして [String] を選択し、ヌル以外の値をユーザに入力すると、そのユーザはすでに設定されている値に一致する名前で ID ストアに対して、ユーザの詳細に示されている属性について認証されます（ACS-RESERVED-Authen-ID-Store）。 • Unsigned Integer 32：ページの [Valid Range From] フィールドと [Valid Range To] フィールドにデータが読み込まれます。 • [IP Address]：ページの [Default Value] フィールドにデータが読み込まれます。これは、IPv4 または IPv6 アドレスにできます。 • Boolean：ページの [Default Value] チェックボックスにデータが読み込まれます。Boolean 属性の値を true に設定すると、パスワードの有効期限ポリシーのグローバル設定を上書きし、ポリシーを非アクティブ化します（ACS-RESERVED-Never-Expired）。 • Date：ページの [Default Value] フィールドにデータが読み込まれ、カレンダー アイコンが表示されます。 • Enumeration：[ID] フィールドと [Value] フィールドにデータが読み込まれ、[Add]、[Edit]、[Replace]、および [Delete] ボタンが表示されます。
Maximum Length	（任意）*String 属性タイプの場合のみ*。属性の最大長を入力します。有効な範囲は 1 ～ 256 です（デフォルト = 32）。
Value Range	（任意）*Unsigned Integer 属性タイプの場合のみ*。 • From：受け入れられる最小整数値を入力します。有効な範囲は 0 ～ 2^31-1（2147483647）です。この値には、[Valid Range To] の値よりも小さい値を指定する必要があります。 • To：受け入れられる最大整数値を入力します。有効な範囲は 0 ～ 2^31-1（2147483647）です。この値には、[Valid Range From] の値よりも大きい値を指定する必要があります。

表 18-10　[Identity Attribute Properties] ページ （続き）

オプション	説明
Default Value	属性のデフォルト値を入力します。 • [String]：最大長まで （UTF-8 標準に従います）。a ～ z の文字、A ～ Z の文字、および 0 ～ 9 の数字を使用できます。 • [Unsigned Integer] 32：0 ～ 2^31-1（2147483647）の範囲の整数。 • [IP Address]：この属性に関連付ける IP アドレスを次の形式で入力します。 – IPv4 アドレス：*x.x.x.x*、ここで *x.x.x.x* は IPv4 アドレス（サブネット マスクなし） – IPv6 アドレス：*x:x:x:x:x:x:x:x*、ここで *x:x:x:x:x:x:x:x* は IPv6 アドレス（サブネット マスクなし） • [Date]：カレンダー アイコンをクリックして、表示されるカレンダーのポップアップで日付を選択します。 • [Boolean Value]：[True] または [False] を選択します。
ID-Value	（任意）*Enumeration 属性タイプの場合のみ。* • [ID]：0 ～ 999 の数字を入力します。 • [Value]：ID の値を入力します。 • [Add] をクリックして、この ID-Value ペアを ID-Value テーブルに追加します。 ID-Value ペアを編集、置換、および削除するには、次の手順を実行します。 • ID-Value テーブルから ID-Value ペアを選択します。 • [ID] および [Value] フィールドを編集するには、[Edit] をクリックします。必要に応じてフィールドを編集します • フィールドを変更したあとで新しいエントリを追加するには、[Add] をクリックします。 • 同じエントリを異なる値で置換するには、[Replace] をクリックします。 • ID-Value テーブルからエントリを削除するには、[Delete] をクリックします。
Attribute Configuration	
Mandatory Fields	この属性を [User Properties] ページの要件にする場合にオンにします。
Add Policy Condition	この属性からカスタム条件を作成する場合にオンにします。このオプションをオンにした場合は、[Policy Condition Display Name] フィールドに名前を入力する必要があります。
Policy Condition Display Name	ポリシー条件の名前を入力します。このページを送信すると、[Policy Elements] > [Session Conditions] > [Custom] ページに条件が表示されます。

内部ユーザ ID 属性の削除

内部ユーザ ID 属性を削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択します。

[Internal Users] ページに [Attributes] リストが表示されます。

ステップ 2　削除する属性の隣にあるチェックボックスをオンにします。

ID 属性を削除すると処理に時間がかかる可能性があるため、削除できるのは一度に 1 つの属性だけです。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のため [OK] または [Cancel] をクリックします。

[Internal Users] ページに [Attributes] リストが表示されます。このとき、削除された属性は表示されません。

関連トピック

- 「内部ユーザ ID 属性の作成、複製、および編集」（P.18-10）
- 「ポリシーおよび ID 属性」（P.3-17）

内部ホスト ID 属性の作成、複製、および編集

内部ホスト ID 属性を作成、複製、および編集するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Hosts] を選択します。

[Internal Hosts] ページに [Attributes] リストが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製する属性の隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更する属性名をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

[Identity Attribute Properties] ページが表示されます。

ステップ 3　必要に応じて、[Identity Attributes Properties] ページのフィールドを変更します。フィールドの説明については、表 18-10 を参照してください。

ステップ 4　[Submit] をクリックします。

内部ホスト属性の設定が保存されます。[Internal Hosts] ページの [Attributes] リストが新しい属性設定で表示されます。

関連トピック

- 「内部ホスト ID 属性の削除」（P.18-13）
- 「ポリシーおよび ID 属性」（P.3-17）

内部ホスト ID 属性の削除

内部ホスト ID 属性を削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal User] を選択します。

[Internal Hosts] ページに [Attributes] リストが表示されます。

ステップ 2　削除する属性の隣にあるチェックボックスをオンにします。

属性を削除すると処理に時間がかかる可能性があるため、削除できるのは一度に 1 つの属性だけです。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のため [OK] または [Cancel] をクリックします。

[Internal Hosts] ページに [Attributes] リストが表示されます。このとき、削除された属性は表示されません。

関連トピック

- 「内部ホスト ID 属性の作成、複製、および編集」（P.18-13）
- 「ポリシーおよび ID 属性」（P.3-17）

[Internal Identity Store] でのユーザへのスタティック IP アドレスの追加

[Internal Identity Store] でユーザにスタティック IP アドレスを追加するには、次の手順を実行します。

ステップ 1　内部ユーザ属性ディクショナリにスタティック IP アドレスを追加するには、次の手順を実行します。

ステップ 2　[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] を選択します。

ステップ 3　[Create] をクリックします。

ステップ 4　スタティック IP 属性を追加します。

ステップ 5　[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。

ステップ 6　[Create] をクリックします。

ステップ 7　ユーザのスタティック IP 属性を編集します。

ローカル サーバ証明書の設定

ローカル サーバ証明書は、ACS サーバ証明書とも呼ばれます。ACS は、ローカル サーバ証明書によってクライアントに識別されます。ローカル サーバ証明書は次のプロトコルまたはインターフェイスによって使用されます。

- SSL/TLS トンネリングを使用する EAP プロトコル
- Web インターフェイス（GUI）を認証する管理インターフェイス

ここでは、次の内容について説明します。

- 「ローカル サーバ証明書の追加」（P.18-15）
- 「サーバ証明書のインポートおよびプロトコルとの関連付け」（P.18-16）
- 「自己署名証明書の生成」（P.18-16）
- 「証明書署名要求の生成」（P.18-17）
- 「CA 署名付き証明書のバインド」（P.18-18）
- 「証明書の編集と更新」（P.18-19）
- 「証明書の削除」（P.18-20）

- 「証明書のエクスポート」（P.18-20）
- 「未処理の署名要求の表示」（P.18-21）

ローカル サーバ証明書の追加

ACS サーバ証明書とも呼ばれるローカル サーバ証明書を追加すると、クライアントで ACS サーバが識別されます。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

[Local Certificates] ページが表示され、表 18-11 の情報が表示されます。

表 18-11　[Local Certificates] ページ

オプション	説明
Friendly Name	証明書に関連付けられている名前。
Issued To	証明書の発行先エンティティ。名前は、証明書のサブジェクトから表示されます。
Issued By	証明書を発行した信頼できるパーティ。
Valid From	証明書の有効開始日。
Valid To (Expiration)	証明書の有効期限日。
Protocol	証明書に関連付けられているプロトコル。

ステップ 2　[Add] をクリックします。

ステップ 3　表 18-12 の説明に従って、[Local Certificate Store Properties] ページに情報を入力します。

表 18-12　[Local Certificate Store Properties] ページ

オプション	説明
Import Server Certificate	クライアント マシンでローカル証明書ファイルを参照し、秘密キーと秘密キーのパスワードをインポートする場合に選択します。「サーバ証明書のインポートおよびプロトコルとの関連付け」（P.18-16）を参照してください。 サポートされている証明書形式には、CER、DER、PEM、Microsoft 秘密キーの独自の形式などがあります。
Generate Self Signed Certificate	自己署名証明書を生成する場合に選択します。「自己署名証明書の生成」（P.18-16）を参照してください。
Generate Certificate Signing Request	証明書署名要求を生成する場合に選択します。「証明書署名要求の生成」（P.18-17）を参照してください。
Bind CA Signed Certificate	CA 証明書をバインドする場合に選択します。RA が要求に署名したあと、返された署名付き証明書を ACS にインストールし、証明書を対応する秘密キーにバインドできます。「CA 署名付き証明書のバインド」（P.18-18）を参照してください。

サーバ証明書のインポートおよびプロトコルとの関連付け

サポートされている証明書形式は、DER または PEM です。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Import Server Certificate] > [Next] を選択します。

ステップ 3　表 18-13 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-13　[Import Server Certificate] ページ

オプション	説明
Certificate File	クライアント マシンでローカル証明書ファイルを参照する場合に選択します。
Private Key File	秘密キーの場所を参照する場合に選択します。
Private Key Password	秘密キーのパスワードを入力します。値の最小長は 0、最大長は 256 です。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）に証明書を関連付ける場合にオンにします。
Management Interface	管理インターフェイスに証明書を関連付ける場合にオンにします。
Allow Duplicate Certificates	同じ CN および同じ SKI を持ち有効開始日、有効期限日、およびシリアル番号が異なる証明書を追加できます。
Override Policy	
Replace Certificate	既存の証明書の内容を、インポートする内容で置き換えるが、既存のプロトコル選択を保持する場合にオンにします。

ステップ 4　[Finish] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

自己署名証明書の生成

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Generate Self Signed Certificate] > [Next] を選択します。

ステップ 3　表 18-14 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-14　自己署名証明書の生成ステップ 2

オプション	説明
Certificate Subject	この要求の生成中に入力された証明書のサブジェクト。[Certificate Subject] フィールドには、英数字を入力できます。最大文字数は 1024 です。このフィールドには、「cn=」というプレフィックスが付けられます。
Key Length	この要求の生成中に入力されたキーの長さ。値は 512、1024、2048、または 4096 です。
Digest to Sign with	ドロップダウン リストから、管理証明書として [SHA1] または [SHA256] を選択します。
Expiration TTL	最大値（正の整数）を日、週、月、および年の単位で選択します。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）に証明書を関連付ける場合にオンにします。
Management Interface	管理インターフェイスに証明書を関連付ける場合にオンにします。
Allow Duplicate Certificates	同じ CN および同じ SKI を持ち有効開始日、有効期限日、およびシリアル番号が異なる証明書を追加できます。
Override Policy	
Replace Certificate	既存の証明書の内容を、インポートする内容で置き換えるが、既存のプロトコル選択を保持する場合にオンにします。

ステップ 4　[Finish] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

証明書署名要求の生成

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Generate Certificate Signing Request] > [Next] を選択します。

ステップ 3　表 18-15 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-15　署名要求の 生成ステップ 2

オプション	説明
Certificate Subject	この要求の生成中に入力された証明書のサブジェクト。[Certificate Subject] フィールドには、英数字を入力できます。最大文字数は 1024 です。このフィールドには、「cn=」というプレフィックスが付けられます。
Key Length	この要求の生成中に入力されたキーの長さ。値は 512、1024、2048、または 4096 です。
Digest to Sign with	ドロップダウン リストから、管理証明書として [SHA1] または [SHA256] を選択します。

ステップ 4　[Finish] をクリックします。

次のメッセージが表示されます。

```
A server certificate signing request has been generated and can be viewed in the
"Outstanding Signing Requests" list.
```

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

CA 署名付き証明書のバインド

このページは、CA 署名付き証明書を CA からの証明書の取得に使用された要求にバインドする場合に使用します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] > [Add] を選択します。

ステップ 2　[Bind CA Signed Certificate] > [Next] を選択します。

ステップ 3　表 18-16 の説明に従って、[ACS Import Server Certificate] に情報を入力します。

表 18-16　CA 署名付き証明書のバインド ステップ 2

オプション	説明
Certificate File	クライアント マシンを参照し、インポートする証明書を選択します。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）に証明書を関連付ける場合にオンにします。
Management Interface	管理インターフェイスに証明書を関連付ける場合にオンにします。
Allow Duplicate Certificates	同じ CN および同じ SKI を持ち有効開始日、有効期限日、およびシリアル番号が異なる証明書を追加できます。
Override Policy	
Replace Certificate	既存の証明書の内容を、インポートする内容で置き換えるが、既存のプロトコル選択を保持する場合にオンにします。

ステップ 4　[Finish] をクリックします。

新しい証明書が保存されます。新しい証明書が含まれた [Local Certificate Store] ページが表示されます。

関連トピック

- 「ローカル サーバ証明書の設定」（P.18-14）
- 「証明書ベースのネットワーク アクセス」（P.4-10）

証明書の編集と更新

既存の自己署名証明書は、削除したり新しい証明書を追加したりしなくても更新できます。これにより、ローカル証明書を使用するサービスは中断されることなく処理を続行できます。ローカル サーバ証明書を更新または延長するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　変更する名前をクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。

ステップ 3　表 18-17 の説明に従って、証明書のプロパティを入力します。

表 18-17　[Edit Certificate Store Properties] ページ

オプション	説明
Issuer	
Friendly Name	証明書に関連付けられている名前。
Description	証明書の説明。
Issued To	*表示のみ。*証明書の発行先エンティティ。名前は、証明書のサブジェクトから表示されます。
Issued By	*表示のみ。*証明書を発行した認証局。
Valid From	*表示のみ。*証明書の有効開始日。X509 証明書は、開始日から終了日までの間（両方の日を含む）だけ有効です。
Valid To (Expiration)	*表示のみ。*証明書の有効最終日。
Serial Number	*表示のみ。*証明書のシリアル番号。
Protocol	
EAP	SSL/TLS トンネリングを使用する EAP プロトコル（EAP-TLS、EAP-FAST、および PEAP）でローカル証明書を使用する場合にオンにします。
Management Interface	ACS で SSL クライアント認証にローカル証明書を使用する場合にオンにします。
Renew Self Signed Certificate	
Certificate Expires On	*表示のみ。*証明書の期限が切れる日。
Renew Self Signed Certificate	期限切れの自己署名証明書の更新を許可する場合に選択します。
Expiration TTL	既存の証明書を延長する日数、月数、週数、または年数。有効なオプションは、[one day]、[one month]、[one week]、および [one year] です。 証明書は最大で 1 年間延長できます。

ステップ 4　[Submit] をクリックして、既存の証明書の有効期間を延長します。

編集した証明書が含まれた [Local Certificate Store] ページが表示されます。

関連項目

- 「ローカル サーバ証明書の設定」（P.18-14）

証明書の削除

証明書を削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　削除する証明書の隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

ステップ 4　確認のため [Yes] または [Cancel] をクリックします。

[Certificate Store] ページが表示されます。このとき、削除した証明書は表示されません。

関連項目

- 「ローカル サーバ証明書の設定」（P.18-14）

証明書のエクスポート

証明書をエクスポートするには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Local Certificates] を選択します。

ステップ 2　エクスポートする証明書の隣にあるチェックボックスをオンにし、[Export] をクリックします。

[Export Certificate] ダイアログボックスが表示されます。

ステップ 3　次のオプションのいずれかを選択します。

- Export Certificate Only
- Export Certificate and Private Key

ステップ 4　[Private Key Password] フィールドに、秘密キーのパスワードを入力します。

ステップ 5　[Confirm Password] フィールドに同じパスワードを入力します。

（注）　秘密キーのエクスポートは、安全な操作ではありません。秘密キーが公開される可能性があるからです。

ステップ 6　[OK] または [Cancel] をクリックします。

関連項目

- 「ローカル サーバ証明書の設定」（P.18-14）

未処理の署名要求の表示

ステップ 1　[System Administration] > [Configuration] > [Local Server Certificates] > [Outstanding Signing Request] を選択します。

[Certificate Signing Request] ページが表示され、表 18-18 で説明されている情報が表示されます。

表 18-18　[Certificate Signing Request] ページ

オプション	説明
Name	証明書の名前。
Certificate Subject	この要求の生成中に入力された証明書のサブジェクト。[Certificate Subject] フィールドには、英数字を入力できます。最大文字数は 1024 です。このフィールドには、自動的に「cn=」というプレフィックスが付けられます。
Key Length	この要求の生成中に入力されたキーの長さ。値は 512、1024、2048、または 4096 です。
Timestamp	証明書が作成された日付。
Friendly Name	証明書に関連付けられている名前。

ステップ 2　[Export] をクリックして、ローカル証明書をクライアント マシンにエクスポートします。

ログの設定

次のメッセージのログ レコードが生成されます。

- アカウンティング メッセージ
- AAA 監査および診断メッセージ
- システム診断メッセージ
- 管理および操作の監査メッセージ

メッセージはツリー階層構造のロギング カテゴリ内に配置されます（「ロギング カテゴリの設定」（P.18-24）を参照）。

ログ メッセージは、ロギング カテゴリおよびメンテナンス パラメータに基づいてローカルまたはリモートに格納できます。

ここでは、次の内容について説明します。

事前に定義されたグローバルな ACS ロギング カテゴリおよび各カテゴリに含まれるメッセージについては、第 19 章「ロギングの概要」を参照してください。

リモート ログ ターゲットの設定

特定のロギング カテゴリのロギング メッセージを受信するように特定のリモート ログ ターゲット（syslog サーバ上だけ）を設定できます。リモート ログ ターゲットの詳細については、第 19 章「ロギングの概要」を参照してください。事前に設定された ACS ロギング カテゴリの詳細については、「ロギング カテゴリの設定」（P.18-24）を参照してください。

新しいリモート ログ ターゲットを作成するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択します。

[Remote Log Targets] ページが表示されます。

ステップ 2　次のいずれかを実行します。

- [Create] をクリックします。
- 複製するリモート ログ ターゲットの隣にあるチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するリモート ログ ターゲットの名前をクリックします。または、変更するリモート ログ ターゲットの名前の隣にあるチェックボックスをオンにして [Edit] をクリックします。

次のいずれかのページが表示されます。

- 新しいリモート ログ ターゲットを作成する場合は、[Remote Log Targets] > [Create]。
- リモート ログ ターゲットを複製する場合は、[Remote Log Targets] > [Duplicate: "*log_target*"]。*log_target* は、ステップ 2 で選択したリモート ログ ターゲットの名前です。
- リモート ログ ターゲットを変更する場合は、[Remote Log Targets] > [Edit: "*log_target*"]。*log_target* は、ステップ 2 で選択したリモート ログ ターゲットの名前です。

ステップ 3　表 18-19 の説明に従って、必須フィールドに入力します。

表 18-19　リモート ログ ターゲットの設定ページ

オプション	説明
General	
Name	リモート ログ ターゲットの名前。名前の最大長は 32 文字です。
Description	リモート ログ ターゲットの説明。説明の最大長は 1024 文字です。
Type	リモート ログ ターゲットのタイプ：[Syslog]（唯一のオプション）。
Target Configuration	
IP Address	リモート ログ ターゲットの IP アドレス（*x.x.x.x* の形式）。
Use Advanced Syslog Options	高度な syslog オプション（ポート番号、ファシリティ コード、および最大長）をイネーブルにする場合にクリックします。
Port	ACS とリモート ログ ターゲット間の通信チャネルとして使用されるリモート ログ ターゲットのポート番号（デフォルト = 514）。このオプションは、[Use Syslog Options] をクリックした場合にだけ表示されます。

表 18-19　リモート ログ ターゲットの設定ページ （続き）

オプション	説明
Facility Code	ファシリティ コード。有効なオプションは次のとおりです。 • LOCAL0（コード = 16） • LOCAL1（コード = 17） • LOCAL2（コード = 18） • LOCAL3（コード = 19） • LOCAL4（コード = 20） • LOCAL5（コード = 21） • LOCAL6（コード = 22、デフォルト） • LOCAL7（コード = 23） このオプションは、[Use Advanced Syslog Options] をクリックした場合にだけ表示されます。
Maximum Length	リモート ログ ターゲット メッセージの最大長。有効なオプションは 200 ～ 1024 です。このオプションは、[Use Advanced Syslog Options] をクリックした場合にだけ表示されます。

ステップ 4　[Submit] をクリックします。

リモート ログ ターゲット設定が保存されます。新しいリモート ログ ターゲット設定が示された [Remote Log Targets] ページが表示されます。

関連項目

- 「リモート ログ ターゲットの削除」（P.18-23）

リモート ログ ターゲットの削除

リモート ログ ターゲットを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択します。

設定されているリモート ログ ターゲットのリストを含む [Remote Log Targets] ページが表示されます。

ステップ 2　削除するリモート ログ ターゲットの隣にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Delete] をクリックします。

次のエラー メッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

ステップ 4　[OK] をクリックします。

[Remote Log Targets] ページが表示されます。このとき、削除したリモート ログ ターゲットは表示されません。

関連項目

- 「リモート ログ ターゲットの設定」（P.18-22）

ローカル ログの設定

ローカル ログ データを保持する最大日数を設定するには、[Local Configuration] ページを使用します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Local Log Target] を選択します。

[Local Configuration] ページが表示されます。

ステップ 2　[Maximum log retention period] ボックスに、ローカル ログ メッセージ ファイルを保管する日数を入力します。<*num*> は入力する日数です。有効なオプションは 1 ～ 365 です （デフォルト = 7）。

（注）　ローカル ログ メッセージ ファイルを保管する日数を減らすと、指定した日数より古いログ メッセージ ファイルは自動的に削除されます。

[Delete Logs Now] をクリックすると、すべての非アクティブなログ ファイルなど、ローカル ログをすぐに削除できます。ログ データの削除の詳細については、「ローカル ログ データの削除」（P.18-24）を参照してください。

ステップ 3　[Submit] をクリックして変更を保存します。

設定が保存され、[Local Configuration] ページが更新されます。

ローカル ログ データの削除

ローカル ログ データを手動で削除するには、[Local Configuration] ページを使用します。この方法を使用して、ローカル ストアがいっぱいになったときに容量を解放できます。ローカル ストアの詳細については、「ローカル ストア ターゲット」（P.19-5）を参照してください。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Local Log Target] を選択します。

[Local Configuration] ページが表示されます。

ステップ 2　[Delete Logs Now] をクリックすると、現在アクティブなログ データ ファイル内のログ データを除くすべてのローカル ログ データ ファイルがすぐに削除されます。

[Local Configuration] ページが更新されます。

ロギング カテゴリの設定

ここでは、次の内容について説明します。

- 「グローバル ロギング カテゴリの設定」（P.18-25）
- 「インスタンスごとのロギング カテゴリの設定」（P.18-30）

親ロギング カテゴリに対して実行されたすべての設定は、そのロギング カテゴリ内の子に影響します。親ロギング カテゴリの子を選択して、個別に設定できます。その子に対する設定は、親ロギング カテゴリまたは他の子に影響しません。

グローバル ロギング カテゴリの設定

グローバル ロギング カテゴリを表示および設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] を選択します。

[Logging Categories] ページが表示されます。このページから、ロギング カテゴリを参照できます。

ステップ 2　設定するロギング カテゴリの名前をクリックします。または、設定するロギング カテゴリの隣にあるオプション ボタンをクリックして [Edit] をクリックします。

ステップ 3　表 18-20 の説明に従って、フィールドに入力します。

表 18-20　[Global: General] ページ

オプション	説明
Configure Log Category	
Log Severity	診断ロギング カテゴリの場合、ドロップダウン リスト ボックスを使用して、重大度レベルを選択します （監査およびアカウンティング カテゴリの場合、重大度は NOTICE だけであり、変更できません）。有効なオプションは次のとおりです。 • [FATAL]：緊急事態。ACS が使用できないため、すぐに対応する必要があります。 • [ERROR]：重大またはエラー状況。 • [WARN]：通常だが、重要な状況 （デフォルト） • [INFO]：通知メッセージ。 • [DEBUG]：診断バグ メッセージ。

表 18-20　[Global: General] ページ （続き）

オプション	説明
Configure Local Setting for Category	
Log to Local Target	ローカル ターゲットへのロギングをイネーブルにする場合にオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、ローカル ターゲットへのロギングはデフォルトでイネーブルであり、ディセーブルにすることはできません。
Local Target is Critical	*アカウンティングおよびAAA 監査（Passed Authentication）ロギング カテゴリ タイプの場合だけ使用できます。*このローカル ターゲットを重大なターゲットにする場合に、このチェックボックスをオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、このチェックボックスはデフォルトでオンであり、オフにすることはできません。このローカル ターゲットは重大なターゲットです。
Configure Logged Attributes	
—	*表示のみ。*すべての属性は、ローカル ターゲットにロギングされます。

設定が完了したら、ステップ 6 に進みます。

ステップ 4　リモート syslog ターゲットを設定するには、[Remote Syslog Target] をクリックし、ステップ 5 に進みます。

ステップ 5　表 18-21 の説明に従って、リモート syslog ターゲットのフィールドに入力します。

表 18-21　[Global: Remote Syslog Target] ページ

オプション	説明
Configure Syslog Targets	
Available targets	使用できるターゲットのリスト。このリストからターゲットを選択して、[Selected Targets] リストに移動できます。
Selected targets	選択されているターゲットのリスト。このリストからターゲットを選択して、[Available Targets] リストに移動し、設定から削除できます。

ステップ 6　[Submit] をクリックします。

設定したロギング カテゴリが示された [Logging Categories] ページが表示されます。

管理および操作の監査メッセージには、次のタイプの監査メッセージが含まれます。

- 設定変更
- 内部ユーザのパスワード変更
- 管理者アクセス
- 操作の監査

操作の監査メッセージの一部は、ローカル ログ ターゲットにロギングされません。ローカル ターゲットにロギングされない管理および操作のログのリストについては、表 18-22 を参照してください。ACS CLI からこれらのログを表示する方法については、「ADE-OS ログの表示」（P.18-29）を参照してください。

表 18-22 に、ローカル ターゲットにロギングされない管理および操作のログのセットをカテゴリ別に示します。

表 18-22　ローカル ターゲットにロギングされない管理および操作のログ

カテゴリ	ログと説明
Process-Management	• ACS_START_PROCESS：ACS プロセスが開始しました。 • ACS_STOP_PROCESS：ACS プロセスが停止しました。 • ACS_START：すべての ACS プロセスが開始しました。 • ACS_STOP：すべての ACS プロセスが停止しました。 • WD_RESTART_PROCESS：ACS プロセスがウォッチドッグによって再起動されました。 • WD_CONFIG_CHANGE：ウォッチドッグ設定がリロードされました。 • ACS_START_STOP_ERROR：ACS プロセスによって開始/停止エラーが報告されました。
DB-Management	• CARS_BACKUP：CARS バックアップが完了しました。 • CARS_RESTORE：CARS 復元が完了しました。 • ACS_BACKUP：ACS DB バックアップが完了しました。 • ACS_RESTORE：ACS DB 復元が完了しました。 • ACS_SUPPORT：ACS サポート バンドルが収集されました。 • ACS_RESET：ACS DB がリセットされました。
File-Management	• ACS_DELETE_CORE：ACS コア ファイルが削除されました。 • ACS_DELETE_LOG：ACS ログ ファイルが削除されました。

表 18-22　ローカル ターゲットにロギングされない管理および操作のログ （続き）

カテゴリ	ログと説明
Software-Management	• ACS_UPGRADE：ACS がアップグレードされました。 • ACS_PATCH：ACS パッチがインストールされました。 • UPGRADE_SCHEMA_CHANGE：ACS スキーマのアップグレードが完了しました。 • UPGRADE_DICTIONARY：ACS ディクショナリのアップグレードが完了しました。 • UPGRADE_DATA_MANIPULATION：ACS アップグレードのデータ処理段階が完了しました。 • UPGRADE_AAC：ACS AAC アップグレードが完了しました。 • UPGRADE_PKI：ACS PKI アップグレードが完了しました。 • UPGRADE_VIEW：ACS ビューのアップグレードが完了しました。 • CLI_ACS_UPGRADE：ACS アップグレードが開始しました。 • CLI_ACS_INSTALL：ACS インストールが開始しました。
System-Management	• ACS_MIGRATION_INTERFACE：ACS 移行インターフェイスがイネーブル/ディセーブルになりました。 • ACS_ADMIN_PSWD_RESET：ACS 管理者パスワードがリセットされました。 • CLI_CLOCK_SET：クロックが設定されました。 • CLI_TZ_SET：タイムゾーンが設定されました。 • CLI_NTP_SET：NTP サーバが設定されました。 • CLI_HOSTNAME_SET：ホスト名が設定されました。 • CLI_IPADDRESS_SET：IP アドレスが設定されました。 • CLI_IPADDRESS_STATE：IP アドレスの状態。 • CLI_DEFAULT_GATEWAY：デフォルト ゲートウェイが設定されました。 • CLI_NAME_SERVER：ネーム サーバが設定されました。 • ADEOS_XFER_LIBERROR：ADE OS Xfer ライブラリ エラー。 • ADEOS_INSTALL_LIBERROR：ADE OS インストール ライブラリ エラー。 • AD_JOIN_ERROR：AD エージェントが AD ドメインに参加できませんでした。 • AD_JOIN_DOMAIN：AD エージェントが AD ドメインに参加しました。 • AD_LEAVE_DOMAIN：AD エージェントが AD ドメインから離脱しました。 • IMPORT_EXPORT_PROCESS_ABORTED：インポート/エクスポート プロセスが中止されました。 • IMPORT_EXPORT_PROCESS_STARTED：インポート/エクスポート プロセスが開始しました。 • IMPORT_EXPORT_PROCESS_COMPLETED：インポート/エクスポート プロセスが完了しました。 • IMPORT_EXPORT_PROCESS_ERROR：インポート/エクスポート プロセス中にエラーが発生しました。

関連項目

- 「インスタンスごとのロギング カテゴリの設定」（P.18-30）

- 「ADE-OS ログの表示」（P.18-29）

ADE-OS ログの表示

表 18-22 に示すログは、ADE-OS ログに書き込まれます。ACS CLI から次のコマンドを使用して ADE-OS ログを表示できます。

show logging system

このコマンドを実行すると、すべての ADE-OS ログが表示されます。出力は次の例のようになります。

```
Sep 29 23:24:15 cd-acs5-13-179 sshd(pam_unix)[20013]: 1 more authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95
user=admin
Sep 29 23:24:34 cd-acs5-13-179 sshd(pam_unix)[20017]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 29 23:24:36 cd-acs5-13-179 sshd[20017]: Failed password for admin from 10.77.137.95
port 3635 ssh2
Sep 30 00:47:44 cd-acs5-13-179 sshd(pam_unix)[20946]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:47:46 cd-acs5-13-179 sshd[20946]: Failed password for admin from 10.77.137.95
port 3953 ssh2
Sep 30 00:54:59 cd-acs5-13-179 sshd(pam_unix)[21028]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:55:01 cd-acs5-13-179 sshd[21028]: Failed password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:35 cd-acs5-13-179 last message repeated 5 times
Sep 30 00:55:39 cd-acs5-13-179 sshd[21028]: Accepted password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:39 cd-acs5-13-179 sshd(pam_unix)[21038]: session opened for user admin by
(uid=0)
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[118] [admin]:
Invoked carsGetConsoleConfig
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[135] [admin]:
No Config file, returning defaults
Sep 30 01:22:20 cd-acs5-13-179 sshd[21038]: Received disconnect from 10.77.137.95: 11:
Connection discarded by broker
Sep 30 01:22:20 cd-acs5-13-179 sshd(pam_unix)[21038]: session closed for user admin
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 02:48:54 cd-acs5-13-179 sshd[22500]: Accepted password for admin from 10.77.137.58
port 4527 ssh2
Sep 30 02:48:54 cd-acs5-13-179 sshd(pam_unix)[22504]: session opened for user admin by
(uid=0)
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
```

所属するモジュールでグループ化されたログを表示できます。たとえば、モニタリングおよびトラブルシューティング ログには文字列 **MSGCAT** が含まれ、デバッグ ログには文字列 **debug** が含まれています。

ACS CLI で次の 2 つのコマンドを入力して、モニタリングおよびトラブルシューティング ログと管理ログを個別に表示できます。

- **show logging system | include MSGCAT**
- **show logging system | include debug**

show logging system | include MSGCAT の出力は次のようになります。

```
Sep 27 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 28 13:00:03 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 06:28:17 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 8363
Sep 29 06:28:28 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 06:31:41 cd-acs5-13-103 MSGCAT58037/admin: Installing ACS
Sep 29 09:52:35 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 32729
Sep 29 09:52:46 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 09:53:29 cd-acs5-13-103 MSGCAT58004/admin: ACS Starting
Sep 29 10:37:45 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 29 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 13:56:36 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:02 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:25 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 30 10:57:10 cd-acs5-13-103 MSGCAT58010/admin: info:[ACS backup] ACS backup completed
```

show logging コマンドの詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html#wp1917127

インスタンスごとのロギング カテゴリの設定

特定の上書きされる ACS インスタンスのカスタム ロギング カテゴリ設定を定義したり、すべてのインスタンスをデフォルトのグローバル ロギング カテゴリ設定に戻したりできます。

インスタンスごとのロギング カテゴリを表示および設定するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択します。

[Per-Instance] ページが表示されます。このページで、展開された個別の ACS インスタンスを表示できます。

ステップ 2　設定する ACS インスタンスの名前に関連付けられているオプション ボタンを選択し、次のいずれかのオプションを選択します。

- 選択した ACS インスタンスの現在のロギング カテゴリ設定を上書きするには、[Override] をクリックします。
- ACS インスタンスに関連付けられた [Logging Categories] ページを表示するには、[Configure] をクリックします。その後、ACS インスタンスのロギング カテゴリを編集できます。フィールドの説明については、「ロギング カテゴリの表示」（P.18-33）を参照してください。
- 選択した ACS インスタンスをデフォルトのグローバル ロギング カテゴリ設定に戻すには、[Restore to Global] をクリックします。

設定が保存され、[Per-Instance] ページが更新されます。

関連項目

- 「インスタンスごとのセキュリティおよびログの設定」（P.18-31）

インスタンスごとのセキュリティおよびログの設定

特定の上書きされる ACS インスタンスまたはカスタム ACS インスタンスについて、ロギング カテゴリ設定の重大度レベルとローカル ログを設定できます。このページを使用して、次のことを行います。

- 特定の ACS インスタンスに設定されているロギング カテゴリのツリーを表示します。
- 特定の ACS インスタンスについてロギング カテゴリの重大度レベル、ログ ターゲット、およびロギングされる属性を設定するページを開きます。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択し、[Configure] をクリックします。

表 18-23 で説明されている [Per-Instance: Configuration] ページが表示されます。

表 18-23　[Per-Instance: Configuration] ページ

オプション	説明
Name	AAA サービス ロギング カテゴリの展開可能なツリー構造。
Edit	選択したロギング カテゴリの [Edit: "*lc_name*"] ページを表示する場合にクリックします。*lc_name* は、ロギング カテゴリの名前です。

ステップ 2　次のいずれかを実行します。

- 設定するロギング カテゴリの名前をクリックします。
- 設定するロギング カテゴリの名前に関連付けられているオプション ボタンを選択し、[Edit] をクリックします。

[Per-Instance: General] ページが表示されます。

このページで、特定の ACS インスタンスについてロギング カテゴリ設定のセキュリティ レベルとローカル ログを設定できます。表 18-24 を参照してください。

表 18-24　[Per-Instance: General] ページ

オプション	説明
Configure Log Category	
Log Severity	リスト ボックスを使用して、診断ロギング カテゴリの重大度レベルを選択します（監査およびアカウンティング カテゴリの場合、重大度は NOTICE だけであり、変更できません）。有効なオプションは次のとおりです。 • [FATAL]：緊急事態。ACS が使用できないため、すぐに対応する必要があります。 • [ERROR]：重大またはエラー状況。 • [WARN]：通常だが、重要な状況 （デフォルト） • [INFO]：通知メッセージ。 • [DEBUG]：診断バグ メッセージ。
Configure Local Setting for Category	
Log to Local Target	ローカル ターゲットへのロギングをイネーブルにする場合にオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、ローカル ターゲットへのロギングはデフォルトでイネーブルであり、ディセーブルにすることはできません。
Local Target is Critical	*アカウンティングおよびPassed Authentication ロギング カテゴリ タイプの場合だけ使用できます。*このローカル ターゲットを重大なターゲットにする場合に、このチェックボックスをオンにします。 管理および操作の監査ロギング カテゴリ タイプの場合、このチェックボックスはデフォルトでオンであり、オフにすることはできません。このローカル ターゲットは重大なターゲットです。
Configure Logged Attributes	
—	*表示のみ。*すべての属性は、ローカル ターゲットにロギングされます。

インスタンスごとのリモート syslog ターゲットの設定

このページは、ロギング カテゴリのリモート syslog ターゲットを設定する場合に使用します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択し、[Configure] をクリックします。

表 18-23 で説明されている [Per-Instance: Configuration] ページが表示されます。

ステップ 2　次のいずれか 1 つの処理を実行します。

- 設定するロギング カテゴリの名前をクリックします。
- 設定するロギング カテゴリの名前に関連付けられているオプション ボタンを選択し、[Edit] をクリックします。

ステップ 3　[Remote Syslog Target] タブをクリックします。

表 18-25 で説明されている [Per-Instance: Remote Syslog Targets] ページが表示されます。

表 18-25　[Per-Instance: Remote Syslog Targets] ページ

オプション	説明
Configure Syslog Targets	
Available targets	使用できるターゲットのリスト。このリストからターゲットを選択して、[Selected Targets] リストに移動できます。
Selected targets	選択されているターゲットのリスト。このリストからターゲットを選択して、[Available Targets] リストに移動し、設定から削除できます。

ロギング カテゴリの表示

特定の ACS インスタンスに設定されているロギング カテゴリのツリーを表示できます。また、特定の ACS インスタンスについてロギング カテゴリの重大度レベル、ログ ターゲット、およびロギングされる属性を設定することもできます。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Per-Instance] を選択し、[Configure] をクリックします。

ステップ 2　表 18-26 の説明に従って、フィールドに入力します。

表 18-26　[Per-Instance: Configuration] ページ

オプション	説明
Name	AAA サービス ロギング カテゴリの展開可能なツリー構造。
Edit	選択したロギング カテゴリの [Edit: "*lc_name*"] ページを表示する場合にクリックします。*lc_name* は、ロギング カテゴリの名前です。

ログ コレクタの設定

ログ データ コレクタを選択し、ログ データの送信を一時停止または再開するには、[Log Collector] ページを使用します。

ステップ 1　[System Administration] > [Configuration] > [Log Configuration] > [Log Collector] を選択します。

[Log Collector] ページが表示されます。

ステップ 2　表 18-27 の説明に従って、[Log Collector] ページのフィールドに入力します。

表 18-27　[Log Collector] ページ

オプション	説明
Log Data Collector	
Current Log Collector	*表示のみ。*ローカル ログ メッセージを送信するマシンを示します。
Select Log Collector	ドロップダウン リスト ボックスを使用して、ローカル ログ メッセージを送信するマシンを選択します。
Set Log Collector	[Select Log Collector] オプションの選択内容に従ってログ コレクタを設定する場合にクリックします。

ステップ 3　次のいずれかを実行します。

- 設定されているログ コレクタへのログ データの送信を一時停止するには、[Suspend] をクリックします。
- 設定されているログ コレクタへのログ データの送信を再開するには、[Resume] をクリックします。

設定が保存され、[Log Collector] ページが更新されます。

ログ メッセージ カタログの表示

[Log Message Catalog] ページは、表示される可能性があるすべてのログ メッセージを表示する場合に使用します。

[System Administration] > [Configuration] > [Log Configuration] > [Log Message Catalog] を選択します。

表 18-28 で説明されているフィールドを含む [Log Message Catalog] ページが表示されます。このページでは、ログ ファイルに記録される可能性があるすべてのログ メッセージを表示できます。

表 18-28　[Log Message Catalog] ページ

オプション	説明
Message Code	*表示のみ。*メッセージに関連付けられている固有のメッセージ コード ID 番号。
Severity	*表示のみ。*メッセージに関連付けられている重大度レベル。
Category	*表示のみ。*メッセージが属するロギング カテゴリ。
Message Class	*表示のみ。*メッセージが属するグループ。

表 18-28　[Log Message Catalog] ページ （続き）

オプション	説明
Message Text	*表示のみ*。英語のメッセージ テキスト（メッセージの名前）。
Description	表示のみ。関連付けられているメッセージを説明する英語のテキスト。

ライセンスの概要

ACS を使用するには、有効なライセンスをインストールする必要があります。ACS では、初めて Web インターフェイスにアクセスしたときに、有効な基本ライセンスをインストールするよう求められます。分散展開では、各 ACS インスタンス（プライマリまたはセカンダリ）に固有の基本ライセンスが必要です。

（注）　分散展開では、各サーバに固有の基本ライセンスが必要です。

ライセンスの種類

表 18-29 に、ACS 5.4 のライセンス サポートを示します。

表 18-29　ACS ライセンスのサポート

ライセンス	説明
基本ライセンス	展開されているすべてのソフトウェア インスタンスと、すべてのアプライアンスに必要です。基本ライセンスをインストールすると、ライセンス制御機能を除くすべての ACS 機能を使用できます。また、すべてのレポート機能がイネーブルになります。基本ライセンスの特性は次のとおりです。 • 各 ACS インスタンス（プライマリとセカンダリ）で必要です。 • すべてのアプライアンスで必要です。 • 最大 500 台の管理対象デバイスを使用した展開をサポートします。 基本ライセンスには次の 3 つのタイプがあります。 • 永続：最大 500 台のデバイスをサポートします。 • 評価：最大 50 台のデバイスをサポートし、90 日で有効期限が切れます。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 評価ライセンスの期限が切れた場合、または間もなく切れる場合は、別の評価ライセンスを使用したり現在のライセンスを延長したりすることはできません。評価ライセンスの期限が切れる前に、永続ライセンスにアップグレードする必要があります。

表 18-29　ACS ライセンスのサポート （続き）

ライセンス	説明
アドオン ライセンス	サポートする管理対象デバイスの数に制限はありません。既存の ACS 永続基本ライセンスが必要です。アドオン ライセンスの評価タイプ ライセンスもあります。 Security Group Access 機能ライセンスは 3 種類です（永続、評価、NFR）。ただし、永続 Security Group Access 機能ライセンスは、永続基本ライセンスがある場合だけ使用できます。 大規模展開ライセンスも、永続基本ライセンスがある場合にだけ使用できます。
評価ライセンス（標準）	標準の集中型レポート機能がイネーブルになります。 • 同じプラットフォームでは再利用できません。 • 評価ライセンスは、プラットフォームごとに 1 つだけインストールできます。追加の評価ライセンスはインストールできません。 • 50 台の管理対象デバイスをサポートします。 • ライセンスのインストール時から 90 日間で期限が切れます。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの追加」（P.18-41）
- 「展開ライセンス ファイルの削除」（P.18-42）

ライセンス ファイルのインストール

有効なライセンス ファイルは、製品に付属している Product Activation Key（PAK; プロダクト アクティベーション キー）を使用して取得できます。ライセンス ファイルを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　ACS Web インターフェイスにログインします。

ACS マシンに初めてログインすると、[Initial Licenses] ページが表示されます。

ステップ 2　[Cisco Secure ACS License Registration] をクリックします。

代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。

ステップ 3　[Install] をクリックして、購入したライセンス ファイルをインストールします。

ACS Web インターフェイスのログイン ページが再度表示されます。これで ACS アプリケーションを使用できます。

（注）　基本永続ライセンスはアップグレードできません。アップグレードできるのは基本評価ライセンスだけです。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの追加」（P.18-41）
- 「展開ライセンス ファイルの削除」（P.18-42）

基本ライセンスの表示

基本ライセンスをアップグレードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Base Server License] を選択します。

[Base Server License] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストが示されます。展開ライセンスのリストについては、「ライセンスの種類」を参照してください。

表 18-30 に、[Base Server License] ページのフィールドを示します。

表 18-30　[Base Server License] ページ

オプション	説明
ACS Deployment Configuration	
Primary ACS Instance	ACS 5.4 Web インターフェイスにログインするときに作成されたプライマリ インスタンスの名前。
Number of Instances	ACS データベース内の ACS インスタンス（プライマリまたはセカンダリ）の現在の数。
Current Number of Configured IP Addresses in Network Devices	ネットワーク デバイス設定の一部として設定したすべてのサブネットワーク内の IP アドレスの総数。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
Maximum Number of IP Addresses in Network Devices	ライセンスでサポートされる IP アドレスの最大数。 • Base License：500 個の IP アドレスをサポートします。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 • Large Deployment：サポートする IP アドレスの数に制限はありません。
Use this link to obtain a valid License File	プロダクト アクティベーション キー（PAK）を使用して有効なライセンス ファイルを生成するために、Cisco.com に移動します。
Base License Configuration	
ACS Instance	ACS インスタンス（プライマリまたはセカンダリ）の名前。
Identifier	基本ライセンスの名前。
License Type	基本ライセンスのタイプ（永続または評価）を指定します。
Expiration	評価ライセンスの有効期限を指定します。永続ライセンスの場合、[Expiration] フィールドに *permanent* と表示されます。
Licensed to	この製品がライセンスされる会社の名前。
PAK	Cisco から受け取ったプロダクト アクティベーション キー（PAK）の名前。
Version	ACS ソフトウェアの現在のバージョン。

ライセンスをアップグレードするインスタンスの隣にあるオプション ボタンを 1 つ以上選択できます。

ステップ 2　[Upgrade] をクリックします。有効なフィールド オプションについては、「基本サーバ ライセンスのアップグレード」（P.18-39）を参照してください。

関連項目

- 「基本サーバ ライセンスのアップグレード」（P.18-39）

基本サーバ ライセンスのアップグレード

基本サーバ ライセンスをアップグレードできます。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Base Server License] を選択します。

[Base Server License] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストが示されます。展開ライセンスのリストについては、「ライセンスの種類」を参照してください。

ステップ 2　ライセンスを選択し、[Upgrade] をクリックします。

[Base Server License Edit] ページが表示されます。

ステップ 3　表 18-31 の説明に従って、フィールドに入力します。

表 18-31　[Base Server License Edit] ページ

オプション	説明
ACS Instance License Configuration	
Version	ACS ソフトウェアの現在のバージョンが表示されます。
ACS Instance	ACS インスタンス（プライマリまたはセカンダリ）の名前が表示されます。
License Type	ライセンス タイプを指定します。
Use this link to obtain a valid License File	代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。
License Location	
License File	[Browse] をクリックして、ライセンス ファイルが格納されているディレクトリに移動し、ファイルを選択します。

ステップ 4　[Submit] をクリックします。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンスの種類」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「展開ライセンス ファイルの追加」（P.18-41）
- 「展開ライセンス ファイルの削除」（P.18-42）

ライセンス機能オプションの表示

既存の展開ライセンスは追加、アップグレード、または削除できます。ページの上部にある設定ペインに、展開情報が表示されます。

[System Administration] > [Configuration] > [Licensing] > [Feature Options] を選択します。

表 18-32 で説明されている [Feature Options] ページが表示されます。

表 18-32　[Feature Options] ページ

オプション	説明
ACS Deployment Configuration	
Primary ACS Instance	ACS 5.4 Web インターフェイスにログインするときに作成されたプライマリ インスタンスの名前。
Number of Instances	ACS データベース内の ACS インスタンス（プライマリまたはセカンダリ）の現在の数。
Current Number of Configured IP Addresses in Network Devices	ネットワーク デバイス設定の一部として設定したすべてのサブネットワーク内の IP アドレスの総数。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
Maximum Number of IP Addresses in Network Devices	ライセンスでサポートされる IP アドレスの最大数。 • Base License：500 個の IP アドレスをサポートします。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 • Large Deployment：サポートする IP アドレスの数に制限はありません。
Use this link to obtain a valid License File	代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。
Installed Deployment License Options	
Feature	• Large Deployment：サポートする管理対象デバイスの数に制限はありません。 • [Security Group Access Control]：Cisco Trusted Server（SGA）管理機能を有効にします。既存の ACS 基本ライセンスが必要です。
Licensed to	この製品がライセンスされる会社の名前。
License Type	ライセンス タイプ（永続または評価）を指定します。
Expiration	次の機能の有効期限。 • 大規模な導入 • SGA
Add/Upgrade	ライセンス機能オプションの表示にアクセスしたりライセンス ファイルを追加したりするには、[Add/Upgrade] をクリックします。
Delete	削除するライセンス機能の隣にあるオプション ボタンを選択し、[Delete] をクリックします。

展開ライセンス ファイルの追加

新しい基本展開ライセンス ファイルを追加するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Feature Options] を選択します。

[Feature Options] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストとそれらの設定が示されます。展開ライセンスのリストについては、「ライセンスの種類」の「アドオン ライセンス」を参照してください。フィールドの説明については、「ライセンス機能オプションの表示」（P.18-40）を参照してください。

ステップ 2　[Add] をクリックします。

[Feature Options Create] ページが表示されます。

ステップ 3　表 18-33 の説明に従って、フィールドに入力し、ライセンスを追加します。

表 18-33　[Feature Options Create] ページ

オプション	説明
ACS Deployment Configuration	
Primary ACS Instance	ACS 5.4 Web インターフェイスにログインするときに作成されたプライマリ インスタンスの名前。
Number of Instances	ACS データベース内の ACS インスタンス（プライマリまたはセカンダリ）の現在の数。
Current Number of Configured IP Addresses in Network Devices	ネットワーク デバイス設定の一部として設定したすべてのサブネットワーク内の IP アドレスの総数。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
Maximum Number of IP Addresses in Network Devices	ライセンスでサポートされる IP アドレスの最大数。 • Base License：500 個の IP アドレスをサポートします。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。 • Large Deployment：サポートする IP アドレスの数に制限はありません。
Use this link to obtain a valid License File	代理店から有効なライセンス ファイルを購入するために、Cisco.com に移動します。
License Location	
License File	[Browse] をクリックして、インストールする購入済みライセンス ファイルの場所を参照し、ファイルを選択します。

ステップ 4　[Submit] をクリックしてライセンス ファイルをダウンロードします。

追加ライセンスを含む [Feature Options] ページが表示されます。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンスの種類」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの削除」（P.18-42）

展開ライセンス ファイルの削除

展開ライセンス ファイルを削除するには、次の手順を実行します。

ステップ 1　[System Administration] > [Configuration] > [Licensing] > [Feature Options] を選択します。

[Feature Options] ページが表示され、ACS の展開設定の説明および使用可能な展開ライセンスのリストとそれらの設定が示されます。展開ライセンスのリストについては、「ライセンスの種類」の「アドオン ライセンス」を参照してください。フィールドの説明については、表 18-32 を参照してください。

ステップ 2　削除する展開の隣にあるオプション ボタンを選択します。

ステップ 3　[Delete] をクリックしてライセンス ファイルを削除します。

関連トピック

- 「ライセンスの概要」（P.18-35）
- 「ライセンスの種類」（P.18-35）
- 「ライセンス ファイルのインストール」（P.18-36）
- 「基本ライセンスの表示」（P.18-38）
- 「展開ライセンス ファイルの追加」（P.18-41）

使用可能なダウンロード

ここでは、ACS Web インターフェイスからダウンロードできるユーティリティとファイルについて説明します。

- 「移行ユーティリティ ファイルのダウンロード」（P.18-43）
- 「UCP Web サービス ファイルのダウンロード」（P.18-43）
- 「サンプル Python スクリプトのダウンロード」（P.18-43）
- 「Rest サービスのダウンロード」（P.18-44）

移行ユーティリティ ファイルのダウンロード

ACS 5.4 の移行アプリケーション ファイルおよび移行ガイドをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Migration Utility] を選択します。

[Migration from 4.x] ページが表示されます。

ステップ 2　[Migration application files] をクリックして、移行ユーティリティを実行する場合に使用するアプリケーション ファイルをダウンロードします。

ステップ 3　[Migration Guide] をクリックして、『*Migration Guide for Cisco Secure Access Control System 5.4*』をダウンロードします。

UCP Web サービス ファイルのダウンロード

このページから WSDL ファイルをダウンロードして、ACS を社内ポータルに統合し、ACS 内部 ID ストアに設定されている ACS ユーザに自分のパスワードの変更を許可できます。UCP Web サービスを使用すると、ユーザは自分のパスワードだけを変更できます。パスワードは、プライマリまたはセカンダリ ACS サーバ上で変更できます。

UCP Web サービスによって、入力した新しいパスワードと ACS でユーザに設定されているパスワード ポリシーが比較されます。新しいパスワードが定義されている基準に準拠している場合、新しいパスワードが有効になります。プライマリ ACS サーバでパスワードを変更すると、そのパスワードは ACS によってすべてのセカンダリ ACS サーバに複製されます。

UCP WSDL ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [User Change Password] を選択します。

[User Change Password (UCP) web service] ページが表示されます。

ステップ 2　次のいずれかをクリックします。

- [UCP WSDL] : WSDL ファイルをダウンロードします。
- [UCP Web application example] : アプリケーション ファイルをダウンロードします。
- [Python Script for Using the User Change Password Web Service] : サンプル Python スクリプトをダウンロードします。

UCP Web サービスの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/ucp.html.

サンプル Python スクリプトのダウンロード

[Scripts] ページには、次のサンプル Python スクリプトがあります。

- UCP Web サービスの使用
- 一括インポートおよびエクスポート処理の自動化

これらのサンプル スクリプトをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Sample Python Scripts] を選択します。

[Sample Python Scripts] ページが表示されます。

ステップ 2　次のいずれかをクリックします。

- [Python Script for Using the User Change Password Web Service] : UCP Web サービスのサンプル スクリプトをダウンロードします。
- [Python Script for Performing CRUD Operations on ACS Objects] : インポートおよびエクスポート処理のサンプル スクリプトをダウンロードします。

ステップ 3　スクリプトをローカル ハード ドライブに保存します。

スクリプトには、インストール手順が付属しています。スクリプトの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/acs_sdk.html

（注）　シスコのテクニカル サポートでは、デフォルトの Python スクリプトだけがサポートされています。変更されたスクリプトはサポートされていません。

Rest サービスのダウンロード

ACS Rest Service を使用すると、ACS データベースからオブジェクトを作成、更新、削除することができます。

（注）　WADL ファイルを読み取るためのコマンドラインを使用して Rest Service をイネーブルにする必要があります。

ACS Rest Service WADL ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Rest Service] を選択します。

[Rest Service] ページが表示されます。

ステップ 2　次のいずれかをクリックします。

- [Common or Identity] : ACS 5.4 Rest インターフェイスでサポートされるオブジェクトの構造を記述する XSD ファイルをダウンロードします。
- [Schema files] : スキーマ ファイルをダウンロードします。
- [SDK Samples] : SDK サンプルをダウンロードします。

Rest サービスの使用方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/rest.html